THE WAY THE COOKIE CRUMBLES?

Norsk implementering av "cookiedirektivet" i et personvernperspektiv.

Universitetet i Oslo

Det juridiske fakultet

Kandidatnummer: 616

Leveringsfrist: 25.11.2011

Til sammen 17 744 ord

24.11.2011

Innholdsfortegnelse

1 INTRODUKSJON 3

1.1 Bakgrunn 3

1.2 Problemstilling 4

1.3 Metode og rettskilder 5

2 COOKIES 6

2.1 Om cookie-begrepet 6

2.2 Bruken av cookies 11

2.2.1 Løsninger på tekniske problem 11

2.2.2 Profilering og reklame 11

2.2.3 Informasjonssikkerhet 13

2.3 Personopplysninger i Cookies 15

2.3.1 Definisjonen av personopplysninger 15

2.3.2 Er IP-adresser personopplysninger? 17

2.3.3 Lagres det personopplysninger i cookies? 19

2.3.4 Behandles det sensitive personopplysninger gjennom cookies? 20

3 COOKIEDIREKTIVET 23

3.1 Presentasjon av direktivet 23

3.2 Reaksjoner fra den europeiske reklameindustrien 24

3.3 Samtykkekravet i Cookiedirektivet 26

3.4 Implementering av samtykkekravet i noen medlemsland 28

3.4.1 Introduksjon 28

3.4.2 Danmark 29

3.4.3 Frankrike 30
3.4.4 Storbritannia 31
3.4.5 Nederland 33

3.5 EU-kommisjonens reaksjoner på (manglende) implementering 34

4 KRAV OM SAMTYKKE TIL Å BEHANDLE PERSONOPPLYSNINGER I NORSK RETT 35

4.1 Introduksjon 35

4.2 Generelle krav til behandling av personopplysninger 36

4.3 Grunnlag for behandling av personopplysninger 37
4.3.1 Lov- og nødvendighetsgrunnlag 37
4.3.2 Samtykke 39

4.4 Tilbakekall av samtykke 46

4.5 Særlig om innstillinger i brukerens nettleser 48

5 NORSK IMPLEMENTERING AV COOKIEDIREKTIVET 50

5.1 Gjeldende relevant lovgivning 50

5.2 Forslag til endringer i ekomloven og ekomforskriften 53

5.3 Tilsyn og håndheving 54

5.4 Reaksjoner på de nye cookiereglene 56

5.5 Tekniske løsninger – personvern gjennom arkitektur? 60

6 AVSLUTNING OG KONKLUSJON 64

7 LITTERATURLISTE 66

8 LISTER OVER TABELLER OG FIGURER M V 74

1 Introduksjon

1.1 Bakgrunn

Det er i dag nærmest umulig å unngå å etterlate seg elektroniske spor[1] om man tar del i en digital hverdag. Informasjonshandel utgjør en voksende del av verdensøkonomien, og kjøp og salg av personopplysninger er en viktig del av dette. Den stadig større rollen personopplysninger spiller for de kommersielle aktørene på internett har ført til et økt behov for å regulere tilgangen disse aktørene har til opplysninger knyttet til den enkelte brukeren. Direktiv 2009/136/EF[2] (som i media fått tilnavnet "cookiedirektivet", et navn jeg også vil bruke her) kan blant annet sees på som et utslag av dette.[3]

Prosessen med å implementere cookiedirektivet i norsk rett er nå i gang. Som en del av implementeringen er det foreslått endringer i ekomloven og ekomforskriften. Dersom de foreslåtte endringene vedtas, vil dette kunne føre til endringer av praksisen med lagring og behandling av cookies. Vern av personopplysninger ved lagring av cookies til kommersiell bruk er ikke direkte drøftet i norsk juridisk teori. Internasjonalt er temaet viet større oppmerksomhet både i juridisk teori og i den offentlige debatten. I forbindelse med forslaget til endring i ekomloven og ekomforskriften er det behov for en løsningsorientert drøfting av hvordan man kan opprettholde et vern av personopplysninger ved lagring av cookies samtidig som man sikrer økonomisk vekst i informasjonssektoren. Problemet ligger blant annet i å komme frem til løsninger som kan implementeres både på det rettslige og det teknologiske plan.

---

[1] Begrepet "elektroniske spor" er drøftet i Mestad (1986) s. 2.
[2] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance.
[3] Den norske oversettelsen av cookie-begrepet er etter ekomforskriften § 7-3 *informasjonskapsel*. Det engelske uttrykket er imidlertidig godt innarbeidet også i den norske debatten, og jeg velger derfor å bruke dette uttrykket videre i oppgaven.

Ifølge Lawrence Lessig er internett bygget på fire forskjellige reguleringssystem: lovregulering, normer, markedet og arkitekturen.[4] Han trekker frem lovreguleringen og arkitekturen som de viktigste systemene, og argumenterer for at regulering gjennom arkitektur kan være vel så effektiv som regulering gjennom lovverk.[5] Dette er særlig relevant for diskusjonen om hvordan cookiedirektivet kan og bør implementeres. Et fungerende samspill mellom lovregulering og teknologisk arkitektur kan komme til å bli nødvendig for en utvikling som ikke går ut over det private individ.

1.2 Problemstilling

I denne oppgaven vil jeg se nærmere på EU-direktiv 136/2009/EF, det såkalte *cookiedirektivet*, og de krav som der stilles til behandling av personopplysninger ved bruk av cookies til kommersielle formål. Jeg vil finne ut i hvilken grad norsk lov er i overensstemmelse med direktivet, og om direktivet eventuelt utløser behov for endring i, eller tillegg til, eksisterende lovgivning på området. Oppgaven vil deles inn i tre hoveddeler. Jeg vil først drøfte hvilke krav direktivet stiller til samtykke til behandling av personopplysninger ved bruk av cookies. Videre vil jeg se nærmere på de tolknings- og implementeringsløsninger som er valgt eller planlagt i noen utvalgte EU-land, og debattene rundt disse løsningene. Deretter vil jeg se på den norske prosessen med å implementere cookiedirektivet. Jeg vil drøfte forslag til endringer i lov og forskrift, høringsuttalelser og reaksjoner fra forskjellige hold. Målsettingen er en samlet vurdering av utfordringer knyttet til implementeringen av cookiedirektivet i norsk rett og hvordan direktivet kan gjennomføres.

---

[4] Lessig (2006) s. 125.
[5] Id. s. 127 flg.

1.3 Metode og rettskilder

I denne fremstillingen vil jeg gjøre rettsdogmatiske analyser av den norske og europeiske rettstilstanden på området for vern av personopplysninger. Hovedfokuset vil være å drøfte personvernet i forbindelse med bruk av cookies til kommersielle formål.

I analysene vil jeg gjøre bruk av både norske og EU-rettslige kilder. Særlig vil følgende EU-direktiver stå sentralt: personverndirektivet,[6] kommunikasjonsverndirektivet[7] og det såkalte cookiedirektivet.[8] Jeg vil i denne forbindelse også trekke frem uttalelser i direktivenes fortaler. Disse har ikke like stor rettskildevekt som direktivets artikler, men bør likevel tillegges betraktelig vekt. Etter EU-grunnlovens artikkel 249, 3. ledd er EU-direktivene bindende for hver medlemsstat (og med dette også EØS-medlemmene) med hensyn til det tilsiktede mål. Det er det å oppnå *formålet* med et direktiv som er bindende. Fortalene gir svært viktige føringer for direktivenes formål, og er derfor viktige å ta i betraktning når man drøfter EU-direktiver.

I forbindelse med EU-lovgivningen vil jeg i utstrakt grad kommentere uttalelser gjort av *Article 29 Data Protection Working Party* (heretter kalt Artikkel 29-arbeidsgruppen). Artikkel 29-arbeidsgruppen en et rådgivende organ som er nedsatt etter personverndirektivet artikkel 29. Gruppens hovedoppgave er å gi råd til EU-kommisjonen om personvernspørsmål. Gruppen består blant annet av representanter for de enkelte medlemslandenes tilsynsmyndigheter på området, og den er frittstående og uavhengig i sine uttalelser. Norge er ikke representert, men møter som observatør i gruppen.[9] Ettersom Norge gjennom EØS-avtalen må implementere EU-reglene om personvern, må arbeidsgruppens rådgivende uttalelser tillegges samme vekt i Norge som i EU-landene. Uttalelsene til Artikkel 29-arbeidsgruppen er i praksis svært viktige for tolkningen av EU-lovgivningen på området for personvern, ettersom arbeidsgruppen er opprettet av EU-

---

[6] Direktiv 95/46/EF.
[7] Direktiv 2002/58/EF.
[8] Direktiv 2009/136/EF.
[9] Johansen (2001) s. 54.

kommisjonen, og sitter på svært stor kompetanse og generelt har høy anseelse. Gruppens innflytelse er imidlertid omstridt, noe blant annet Google indikerte[10] i forbindelse med Arbeidsgruppens uttalelse om personvern i tilknytning til bruk av søkemotorer.[11]

Den norske personopplysningsloven, ekomloven, og tilhørende forskrifter og forarbeider vil videre være viktige gjenstander for drøftelsen. Også enkelte vedtak truffet av Personvernnemnda vil bli trukket inn. De norske rettskildene vil være utgangspunktet for drøftelsen om den norske implementeringen av EU-direktivet.

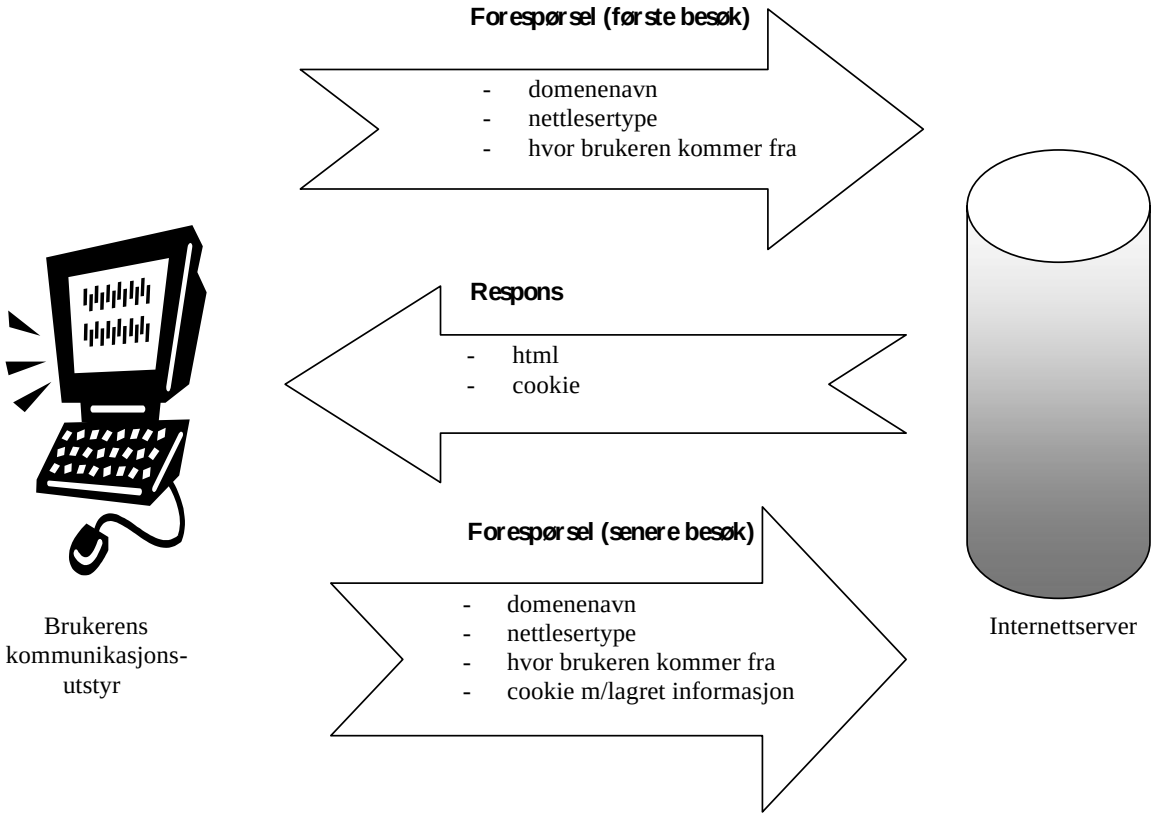
2 Cookies

2.1 Om cookie-begrepet

En *cookie*, eller *http-cookie*, er teknisk sett en kort tekststreng som sendes fra en nettside til harddisken som er i bruk når en bruker besøker nettsiden. Denne tekststrengen lagres i brukerens harddisk, og sendes så tilbake til den nevnte nettsiden hver gang brukeren på nytt besøker siden.[12] Dette er illustrert i figur 1. Http er protokollen som overser forespørsler og respons mellom datamaskiner og servere. Den utgjør grunnlaget for kommunikasjon gjennom World-Wide Web på internett. Denne protokollen er tilstandsløs, og det er dette cookies i utgangspunktet gjør noe med.[13] Uten cookies ville en server ikke være i stand til å relatere en forespørsel fra en klient med en tidligere forespørsel fra samme klient.[14] Ved å sette http-cookies på nettsider, kan man kapsle inn informasjon om når, hvor ofte og hvordan nettbrukere kommuniserer med, eller besøker, et nettsted.[15]

---

[10] Fleischer (2007).
[11] Article 29 Data Protection Working Party: WP 148 (2008).
[12] Tirtea (2011) s. 2 flg.
[13] Id.
[14] Id.
[15] Dwyer (2009) s. 1.



Figur 1. **Hvordan fungerer cookies?**

Det finnes forskjellige typer cookies. Inndelingen kan gjøres etter et *tidsperspektiv*[16] eller et *adgangsperspektiv*.[17] Dersom man deler cookies inn etter *tidsperspektivet*, skiller man mellom midlertidige cookies (*session cookies*) og varige cookies (*persistent cookies*). Midlertidige cookies lagres kun i løpet av et enkelt nettsidebesøk, og vil opphøre å eksistere når man lukker nettleseren.[18] Slik kan nettbutikker for eksempel i løpet av brukerens besøk på deres nettsider lagre informasjon om hva de har lagt i sin virtuelle handlekurv, uten at denne informasjonen går tapt hvis brukeren klikker seg videre til et nytt produkt. Varige cookies lagres permanent, eller opphører å eksistere ved det tidspunkt de er

[16] Tirtea (2011) s. 5.
[17] Id. s. 3.
[18] Id. s. 5.

innstilt til å opphøre eller dersom brukeren selv manuelt går inn og sletter dem.[19] Svært mange nettsteder velger å bruke varige cookies fremfor midlertidige cookies, ettersom de da kan beholde for eksempel innholdet i en handlekurv til neste gang brukeren besøker nettsidene deres. I tillegg er varige cookies mye mer fordelaktige å bruke til profileringsformål, noe jeg vil komme tilbake til i kapittel 2.2.2.

Deler man cookies inn etter *adgangsperspektivet*, skiller man mellom førstepartscookies og tredjepartscookies.[20] Førstepartscookies er cookies som settes av eieren av det besøkte nettstedet, mens tredjepartscookies er cookies som settes av en tredjepart etter å ha blitt henvist til brukeren av førsteparten, det vil si eieren av den besøkte nettsiden. Nettstedets administrator har i dette siste tilfellet ikke selv kontroll over cookiene. Ved å inkludere tredjepartsinnhold på siden sin, henviser administratoren av nettstedet disse tredjepartene til å sette cookies i utstyret til brukerne sine.[21] Tredjepartscookies er, forklart på en annen måte, cookies som er satt av en annen server enn den som vises i nettleseren til brukeren som besøker et bestemt nettsted.

Figur 2 viser de ulike typene cookies sett i relasjon til personvernet. Her er lagringen av cookies inndelt etter lagrings- og adgangsperspektivene, og rangert etter farene som de forskjellige typene cookies kan utgjøre for personvernet. Midlertidige førstepartscookies er som regel ikke problematiske, ettersom disse stort sett er cookies som settes av tekniske nødvendighet. Midlertidige tredjepartscookies og varige førstepartscookies kan imidlertid i enkelte tilfeller tenkes å by på personvernproblemer. Varige tredjepartcookies er nok den mest problematiske typen cookie. Disse settes som regel ikke av sikkerhetsmessige eller teknisk-praktiske grunner, men ofte med markedsføring og brukerprofilering som formål.

---

[19] Id. s. 5.
[20] Id. s. 3.
[21] Id.

		ADGANG TIL INNHOLDET I COOKIES	
		Førstepart (nettsiden som besøkes)	**Tredjepart (en annen enn nettsiden som besøkes)**
LAGRINGSTID	**Midlertidig**	***OK***	***"GRÅSONE"***
	Varig	***"GRÅSONE"***	***IKKE OK***

Figur 2. **Forskjellige typer cookies i et personvernperspektiv.**

De såkalte *sporingscookiene* brukes ofte til slike reklameformål. Disse lagres i en brukers nettleser for å spore hans eller hennes nettvaner, og for slik å kunne plassere bedre rettet reklame på denne brukerens søkemotor, nettleser eller ofte besøkte nettsider.[22] Sporingscookies følger brukerens aktivitet på bestemte nettsider, fra han eller hun klikker seg inn på siden inntil de forlater den. Informasjon som loggføres kronologisk, er for eksempel hvor brukeren har kommet til nettstedet fra, hvilke sider på nettstedet brukeren besøker og hvor lenge, og hvilke søk brukeren gjør internt på nettsiden. Hittil har de fleste cookiene som lagres i en brukers utstyr, kunnet slettes av brukeren dersom de ikke er ønskelige. I løpet av de siste årene har det imidlertid blitt utviklet noen særlig motstandsdyktige typer av cookies som det er vanskelig eller umulig for brukeren å slette.

[22] Sipior (2011) s. 1.

Utviklingen og bruken av såkalte *supercookies* har eksplodert. *Flash cookies* er den vanligste typen supercookies. Disse lagres på nettsider som bruker Adobe Flash, et program som blant annet muliggjør bruk av spesielle typer video, animasjon og interaktivitet på nettsider. Flash-formatet er blitt svært vanlig, og de aller fleste PC'er som kan kobles opp mot internett støtter derfor Flash. I alle slike programmer lagres Flash cookies, som er spesielt motstandsdyktige. De lagres ikke i nettleseren og kontrolleres ikke av denne, de lagres i selve Flash-programmet. Dermed vil ikke Flash cookies bli slettet når en bruker går inn i nettleserinnstillingene sine og sletter "alle" cookies. I tillegg har Flash cookies mye større lagringskapasitet enn vanlige http-cookies, og de har i utgangspunktet ingen utløpsdato. Brukeren blir heller ikke varslet om at denne typen cookies lagres. Dette gjør kontrollen med disse cookiene fra brukersiden svært vanskelig, og man får blant annet problemer med kravet om brukerens samtykke til lagring.[23] *Evercookies* er en enda mer motstandsdyktig type cookie som ble lansert i september 2010.[24] Denne typen cookies lagres i nettleseren, men er ekstremt motstandsdyktig, ettersom cookie-innholdet lagres i alle lagringsmekanismene som er tilgjengelige i nettleseren. Dermed kan en cookie enkelt og raskt gjenskapes dersom brukeren sletter den fra sin nettleser, ettersom den samme cookien er å finne et annet sted i nettleseren.[25]

Utviklingen av særlig motstandsdyktige typer cookies utgjør en stor trussel for brukernes personvern, ettersom de verken blir informert om, eller er merkbare for brukeren. Det er dermed umulig for brukeren å nekte samtykke eller å slette cookiene i etterkant av lagring.

---

[23] Tirtea (2011) s. 8.
[24] Kamkar (2008).
[25] Id.

2.2 Bruken av cookies

2.2.1 Løsninger på tekniske problem

Cookies har vært i bruk på internettet siden juni 1994. Programmereren Lou Montulli, som arbeidet for Netscape, utviklet teknologien som en løsning på problemet med at man ikke hadde noen metoder for å registrere at tilbakevendende brukere hadde besøkt nettsider fra før.[26] Før cookies kom i bruk, måtte enhver handelstransaksjon gjennomføres fra begynnelse til slutt hver eneste gang den ble gjort, selv om det var snakk om små, repetetive transaksjoner. Dette var tidkrevende og sannsynligvis også nokså irriterende for tilbakevendende brukere.

Det var altså ikke med informasjonshandel (per se) som mål at praksisen med å sette cookies startet, og det er fortsatt mange viktige bruksområder for cookies utenom den rene brukerprofileringen som så mange bekymrer seg for. Cookies brukes blant annet til å hente inn informasjon på nytt dersom et vindu eller en nettside uheldigvis skulle lukkes, og til å sette språkinnstillinger basert på IP-adressers lokalisering, så brukere umiddelbart kan lese en nettside på sitt eget språk. Det er også cookies som muliggjør lagring og autentisering av brukernavn og passord, bokmerkelagring og lagring av preferanser og loggdata.[27] Disse små tekstfilene har altså mange viktige bruksområder ved siden av brukerprofilering.

2.2.2 Profilering og reklame

Informasjonshandel og reklame på internett er en viktig inntektskilde for et stort antall internettaktører og utgjør en viktig faktor for økonomisk vekst i internettnæringen.[28] Ved å betale for å få sette tredjepartscookies hos forskjellige nettsider, utvikler bedrifter og internettforetak sine egne sett av brukerprofiler. Disse baserer seg på hvilke linker og reklamer brukerne har klikket seg videre til, samt hvilke nettsteder de besøker og hvor lang tid de tilbringer på hvert nettsted.

---

[26] Schwartz (2001).
[27] Tirtea (2011) s. 2.
[28] Article 29 Data Protection Working Party: WP 171 (2010) s. 4.

Det har de siste årene utviklet seg et stort marked for utvikling av brukerprofiler og plassering av annonser gjort av profesjonelle reklamenettverk. Reklamenettverkene spesialiserer seg på brukerprofilering på nett. De utvikler forskjellige kategorier av brukerprofiler som de så bruker når de plasserer annonser for kundene sine, som er annonsører og utgivere av forskjellige slag. Reklamer plasseres på forskjellige nettsider som formodentlig har brukere som tilsvarer annonsørenes målgrupper.[29] Slik kan bedrifter kjøpe svært treffsikre annonseplasser ut fra reklamenettverkenes profiler, som ofte er basert på informasjon fra tredjepartscookies. En særlig stor aktør på dette markedet er Google, som i tredje kvartal i 2011 fikk 96% av inntektene sine fra reklametjenester.[30] Selskapet dominerer på verdensbasis med sine tjenester *Google Analytics*, *AdWords* og *AdSense*. De eier også reklamegiganten *DoubleClick*, som er et av de største reklamenettverkene i verden.

For bedre å kunne forstå hvordan reklamenettverkene i praksis opererer, vil jeg kort presentere Googles mest populære tjenester for reklame og annonsering. *Google Analytics* er en gratis tjeneste for eiere av nettsteder som ønsker å vite mer om hvordan nettsider brukes.[31] Tjenesten fører statistikk over svært mange nettsider, og kan også spore brukere fra andre sider og søkemotorer, samt spore klikk på annonselinker og respons på markedsføring over e-post. Google Analytics rapporterer om hvilke sider på et nettsted en bruker har besøkt, hvor lenge han eller hun har besøkt hver side, fra hvilken nettside brukeren kom fra og hvor han eller hun befinner seg. Slik kan de gi kundene sine svært nyttige pekere til hvordan de bør sette sammen nettsidene sine og hvor og hvordan de bør annonsere på nettet. *Google AdSense* er en tjeneste som tilbyr nettsideeiere å tjene penger på plassering av atferdsrettede Google-reklamer på nettsidene deres.[32] AdSense bruker cookies for å lagre informasjon på en liknende måte som det Google Analytics gjør. *Google AdWords* er den største reklametjenesten til Google. Tjenesten gir annonsører muligheten

---

[29] Id. (2010) s. 3.
[30] Google Inc. (2011).
[31] http://www.google.com/analytics/.
[32] http://www.google.no/intl/en/ads/.

til å velge seg en rekke ord som skal forbindes med deres annonse, som dukker opp i reklamefeltet til Googles søkemotor når en bruker søker etter innhold ved å bruke noen av disse ordene.[33]

Også innenfor e-handelen brukes cookies hyppig til profileringsformål. En enkelt aktør kan la opptil flere tredjeparter sette cookies på deres nettsider. Et eksempel på dette er jeansgiganten Levi's. Ifølge en undersøkelse fra 2009,[34] delte Levi's sin amerikanske nettbutikk opplysninger om sine kunders atferd med hele åtte forskjellige tredjeparter – enten i form av opplysninger lagret i cookies eller ved såkalte *web beacons*, som jeg vil komme tilbake til i kapittel 2.3.3.

Det er ikke bare de største aktørene som benytter seg av de nevnte reklamenettverkstjenestene. De aller fleste som har en nettside eller driver profesjonell internettaktivitet setter cookies. Svært mange av disse benytter seg også av reklamenettverkstjenester som de ovenfor nevnte Google-tjenestene. Det kan være snakk om internettbutikker, nettaviser og små blogger, eller store sosiale nettverk, som Facebook og LinkedIn. Det er imidlertid ikke alle som setter cookies med gode hensikter. Dette kan gå ut over brukerens informasjonssikkerhet i tillegg til hans eller hennes (generelle) personvern.

2.2.3 Informasjonssikkerhet

Det er mange teknikker som brukes av uvedkommende tredjeparter for å angripe cookies eller utnytte dem til ulovlige formål. Blant de vanligste finner man *phishing, cache sniffing, cookie sniffing* og *web beacons.*[35] *Phishing* er en teknikk som brukes for å "fiske" informasjon man ikke har tilgang til, som for eksempel passord, brukernavn, og bankkortinformasjon. En måte å gjøre dette på, er å fiske etter informasjon som ligger i

---

[33] Id.
[34] Dwyer (2009) s. 7.
[35] Dwyer (2009) s. 7

cookies lagret på brukerens datautstyr.[36] Ved såkalt *cache sniffing* og *cookie sniffing*, sporer en tredjepart opp cookies som er lagret på brukerens datautstyr, og kan blant annet kopiere innholdet i cookiene.[37] Ved *session hijacking* bruker en tredjeperson informasjon fra cookies til å skaffe seg påloggingsinformasjon til forskjellige typer påloggingstjenester. En såkalt *web beacon* er en tom bildefil som brukes for å spore en brukers navigering gjennom én eller flere nettsider. Alene brukes web beacons av tredjeparter til å overvåke nettbruk, men disse filene kan også brukes sammen med cookies for å lagre og behandle opplysninger om denne nettbruken.[38]

Det er altså mange forskjellige metoder for å spore opp og kopiere innholdet i cookies lagret på brukerutstyr. Dette er en stor trussel både mot personvernet og informasjonssikkerheten. Brukere kan for eksempel bli utsatt for svindel og identitetstyveri som et resultat av lagring av cookies, og slik lagring kan også gjøre det lettere å hacke seg inn på brukeres utstyr. Det kan imidlertid argumenteres for at dette er trusler som ikke bare er knyttet til lagring av cookies, og at brukere løper den samme risikoen dersom de ikke godtar lagring av cookies. Det er det mer generelle vernet om personopplysninger som er fokus for denne drøftelsen, og ikke vernet om informasjonssikkerhet. Likevel er det viktig å være klar over at farene ved bruken av cookies strekker seg lenger enn til krenkelser av personvernet.

---

[36] Cannon (2005) s. 82.
[37] Id.
[38] Dwyer (2009) s. 2.

2.3 Personopplysninger i Cookies

Cookies kan, ifølge Hannemyr,[39] i prinsippet inneholde hva som helst.[40] Det er likevel hovedsakelig informasjon om en persons aktivitet og valg på internett som er å finne i cookies. Dette kan være alt fra språkpreferanser og valg av grafikk og oppsett for nettsider til søkeord i Google og Bing. Cookiedirektivet, som jeg vil presentere nærmere i kapittel 3, opererer med den forutsetning at cookies defineres som personopplysninger. Jeg ser likevel grunn til å drøfte denne konklusjonen innledningsvis, ettersom den kanskje kan hevdes å ikke være like etablert i norsk rett som i EU-retten. Jeg mener også at det er nødvendig for drøftingen i de følgende kapitlene å være oppmerksom på bakgrunnen for dette valget, og det at tolkningen som er lagt til grunn i direktivet ikke er det eneste tolkningsalternativet.

2.3.1 Definisjonen av personopplysninger

Personopplysninger er ifølge personopplysningsloven § 2 nr. 1 "opplysninger og vurderinger som kan knyttes til en enkeltperson". I forarbeidene er personopplysningsbegrepet drøftet mer inngående, og disse diskusjonene er veiledende for tolkningen av begrepet i henhold til norsk lov. Ifølge forarbeidene er enkeltpersonen det refereres til, den registrerte/brukeren.[41] Definisjonen inkluderer både direkte og indirekte tilknytning.[42] Bruken av uttrykket "*kan* knyttes til", tilsier at den behandlingsansvarlige ikke nødvendigvis må praktisere en slik kobling av opplysningene til enkeltpersoner. Det er tilstrekkelig at den behandlingsansvarlige har muligheten til å foreta koblingen for at man definerer opplysningene som personopplysninger.[43]

Eksempler på opplysninger som direkte eller indirekte kan bidra til identifisering, er "(…) navn, identifikasjonsnummer eller et annet kjennetegn som er spesielt for personens

---

[39] Rapport skrevet for Personvernnemnda av universitetslektor Gisle Hannemyr ved Institutt for informatikk ved universitetet i Oslo i forbindelse med sak PVN 2006-04 – Microsoft Windows XP. Rapporten er referert i Personvernnemndas vedtak.
[40] PVN 2006-04 – Microsoft Windows XP.
[41] Ot.prp. nr 92 (1998-1999) s. 102 flg.
[42] Id.
[43] Id.

fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sosiale identitet(…)".[44] Disse eksemplene innebærer en nokså vid tolkning av tilknytningskriteriet, som for eksempel favner videre enn tilsvarende kriterier i forvaltningsloven.[45] Også opplysninger som for den behandlingsansvarlige fremstår som anonymiserte, skal kunne defineres som personopplysninger hvis der er tilknytningspunkter som gjør identifisering mulig. Det er uttalt i Ot.prp. nr. 92 at "alle hjelpemidler som det er rimelig å tro at noen kan komme til å anvende for identifiseringsformål", skal tas i betraktning.[46]

Den norske definisjonen av personopplysning er basert på definisjonen i personverndirektivet artikkel 2 (a):[47]

> " 'personal data' shall mean any information relating to an identified or identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"[48]

Direktivets definisjon er mer utfyllende enn den norske, og det er uttrykkelig nevnt at også opplysninger som indirekte kan knyttes til en person, er personopplysninger. Særlig er det opplysninger som refererer til identifikasjonsnummer eller andre attributter som kan knyttes til en person. Det ligger imidlertid mange tolkningsanvisninger i forarbeidene til den norske personopplysningsloven, og tar man disse i betraktning er ikke forskjellene særlig store mellom de to regelsettene.

---

[44] Id.
[45] Id.
[46] Id.
[47] Schartum (2006) s. 14.
[48] Direktiv 95/46/EF artikkel 2 (a).

2.3.2 Er IP-adresser personopplysninger?

Når cookies lagres i kommunikasjonsutstyr som har såkalte "unike identifikatorer", tillater dette sporing av utstyrets brukere.[49] Dette kan skje ved at informasjon om brukerens IP-adresse lagres i cookiene. Det er derfor nødvendig å drøfte om IP-adresser kan defineres som personopplysninger før spørsmålet om det er personopplysninger i cookies kan drøftes.

En IP-adresse er et unikt nummer som er tilknyttet enhver elektronisk enhet som er tilkoblet internett.[50] Når man besøker en nettside, er IP-adressen til oppkoblingen man bruker, synlig for sidens administratorer. Videre kan det for enkelte IP-adresser også være mulig å estimere nettverksutstyrets geografiske lokalisering og hvilken nettverksleverandør adressen er tilknyttet.[51] Det er kun internettleverandørene som sitter med fullstendig informasjon om hvilke internettkunder som "eier" de forskjellige IP-adressene. Det er på det rene at internettleverandørene, ved behandling av sine kundekonti, knytter IP-adresser til kundene sine. I forarbeidene til personopplysningsloven er det uttalt at selv en begrenset tilgang, som tilgangen til "opplysninger som vedkommendes internettleverandør sitter inne med", er tilstrekkelig til at man definerer opplysningene som personopplysninger.[52]

Spørsmålet er om IP-adresser med dette må sies å kunne knyttes til enkeltpersoner. Det er uttalt i personopplysningslovens kommentarutgave at blant annet Statistisk Sentralbyrå og Datatilsynet har operert etter en antakelse om at dersom opplysninger kan "føres tilbake til en enhet på mindre enn fire personer", defineres de som personopplysninger.[53] Forfatterne antyder at dette er en løsning også lovgiverne lettere vil kunne gå for "i situasjoner hvor personverntrusselen er fremtredende".[54] Hensynet til privatlivets fred, som personopplysningsloven etter formålsbestemmelsen er ment å beskytte, tilsier imidlertid at

---

[49] Article 29 Data Protection Working Party: WP 171 (2010) s. 9.
[50] Rasmussen (2007) s. 165.
[51] Article 29 Data Protection Working Party: WP 148 (2008) s. 6.
[52] Ot.prp. nr. 92 (1998-1999) s. 101.
[53] Johansen (2001) s. 69.
[54] Id.

man bør kunne inkludere også en større familie som en enhet det kan knyttes personopplysninger til.[55] Dette kan tyde på at IP-adresser som for eksempel kan knyttes til utstyr som brukes av en familie, bør anses som personopplysninger. Det er ofte slik at en enhet er i bruk av flere personer, enten det er snakk om en arbeidsstasjon på en skole, en brukermaskin på et bibliotek eller en enhet tilhørende en arbeidsplass som er tilgjengelig for flere av arbeidstakerne. I slike tilfeller er det usikkert hvilket enkeltindivid opplysninger knytter seg til, og man kan vanskelig hevde at IP-adressen knytter seg til én bestemt person. Likevel er den største andelen av maskiner og annet kommunikasjonsutstyr i bruk av én eller noen få definerte personer. For eksempel er det ofte snakk om en enkeltpersons personlige laptop eller mobiltelefon. I norsk praksis synes IP-adressen å være definert som en personopplysning. Dette er antydet i Personvernnemndas sak fra 2006 om Microsofts automatiske oppdateringer.[56] Nemnda hevdet at IP-adressen kan benyttes til personidentifikasjon, men at dette forutsetter adgang til internettleverandørens logger.[57] Videre ble det uttalt eksplisitt i Personvernnemndas sak fra 2009 om Altinns loggføring av IP-adresser at disse er personopplysninger.[58] Artikkel 29-arbeidsgruppen har i sin uttalelse fra 2000 også hevdet at IP-adresser må anses som personopplysninger.[59] Dette er videre forutsatt i uttalelsen deres fra 2007 om personopplysningskonseptet.[60]

Det synes klart at det er enighet både i norsk rett og EU-retten om at IP-adresser ikke alltid kan karakteriseres som personopplysninger. Vanskelighetene som ligger i å skille mellom IP-adresser som knytter seg til enkeltpersoner, og de om ikke gjør det, medfører imidlertid at man tvinges til konsekvent å behandle alle IP-adresser som om de var personopplysninger.

---

[55] Personopplysningsloven § 1.
[56] PVN 2006-04 Microsoft Windows XP.
[57] Id.
[58] PVN 2009-14 Altinn.
[59] Article 29 Data Protection Working Party: WP 37 (2000).
[60] Article 29 Data Protection Working Party: WP 136 (2007) s. 16.

2.3.3 Lagres det personopplysninger i cookies?

For at cookies skal kunne vurderes etter den norske personopplysningsloven, må det som i kapittel 2.3.2. stadfestes om cookies inneholder "opplysninger og vurderinger som kan knyttes til en enkeltperson", jamfør kapittel 2.3.1. Spørsmålet er om opplysningene som lagres i cookies kan knyttes til enkeltpersoner. Informasjonsinnholdet i cookies er svært variert. Det kan for eksempel dreie seg om enkle "Session ID"-cookies[61] eller sertifiseringscookies, men det kan også dreie seg om mer omfattende analysecookies satt av tredjeparter. Det er klart at ikke all informasjon som lagres i cookies, kan knyttes til en enkeltperson.

Selv om det i personverndirektivets artikkel 2(a) nevnes at opplysningen enten direkte eller indirekte må kunne knyttes til en person for å være en personopplysning, nevnes der ingenting konkret om hvilke formkrav som stilles til opplysningen. Direktivet er imidlertid ment å være teknologinøytralt, og det bør ikke ha noen betydning hvorvidt cookies ikke er direkte nevnt, så lenge teknologien kan brukes til behandling av personopplysninger.[62] I en uttalelse fra 2009 om atferdsrettet reklame[63] har artikkel 29-arbeidsgruppen mer konkret kommet inn på spørsmålet om hvorvidt cookies er å anse som personopplysninger. De hevder at behandlingen av "unike identifikatorer" ved lagring av cookies kan knyttes til en person og dermed er å anse som behandling av personopplysninger.[64] Informasjonen som ligger i en cookie er unik fordi den knytter seg til nettleseren eller kommunikasjonsutstyret den er lagret i. Disse vil alltid ha unikt identifiserbare serienummer eller andre unike kjennemerker. Ettersom cookiene lagres i en elektronisk enhet som er tilkoblet internett, kan alle typer cookies også knyttes til en IP-adresse. Arbeidsgruppen hevder i sin uttalelse om personvern og søkemotorer at cookies muliggjør en mer nøyaktig identifisering av

---

[61] "Session ID-cookies" er cookies som lagrer opplysninger om en internettøkt i forbindelse med nettverkskommunikasjonen.
[62] Direktiv 95/46/EF, fortale nummer 27.
[63] Article 29 Data Protection Working Paper: WP 171 (2010) s. 9.
[64] Id.

brukeren enn det IP-adresser gjør.[65] Gjennom cookies kan man spore dynamiske IP-adresser[66] fra en økt til en annen dersom cookiene ikke slettes etter hver økt.[67] I tillegg til de metodene som allerede er nevnt, kan cookies blant annet brukes til å skaffe påloggingsinformasjon til tjenester på nett, noe som kan føre til identifikasjon av enkeltindivider (dette vil bli tatt opp i kapittel 3.1.).

Muligheten til blant annet å identifisere fysiske personer gjennom sporingen av IP-adresser tilsier at cookies må defineres på tilsvarende måte som IP-adresser. Selv om cookies ikke alltid kan knyttes til en person, må man behandle alle cookies som personopplysninger, ettersom man vanskelig kan skille mellom de cookies som fører til identifikasjon og de som ikke gjør det. Utgangspunktet for min videre fremstilling av tema er derfor at cookies defineres som personopplysninger.

2.3.4 Behandles det sensitive personopplysninger gjennom cookies?

Ettersom jeg anser cookies for å være personopplysninger, må det videre stilles spørsmål ved om cookies i tillegg kan defineres som sensitive personopplysninger.
For denne typen opplysninger er kravene til behandling og brukersamtykke strengere. Dette følger blant annet av personopplysningsloven § 9 og personverndirektivet artikkel 8, hvor det stilles tilleggskrav til behandling av sensitive personopplysninger. Blant annet må man etter personopplysningsloven § 33 ha konsesjon fra Datatilsynet for å behandle sensitive personopplysninger. Disse er i personopplysningsloven § 2 (8) definert som følgende:

---

[65] Article 29 Data Protection Working Party: WP 148 (2008) s. 7.
[66] En dynamisk IP-adresse er en IP-adresse som kan konfigureres på nytt av brukeren.
[67] Article 29 Data Protection Working Party: WP 148 (2008) s. 7.

"Opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
c) helseforhold,
d) seksuelle forhold,
e) medlemskap i fagforeninger."

Denne bestemmelsen bygger på personverndirektivet artikkel 8 nr.1,[68] men det er i den norske versjonen lagt til i bokstav (b) at opplysninger om en persons tidligere straffeforhold er sensitive. Dersom cookies skal anses å være sensitive personopplysninger, må det kunne knyttes informasjon av den karakter som er nevnt i § 2 (8) til cookiene. Dermed må man se nærmere på det konkrete informasjonsinnholdet i cookies. Som nevnt i kapittel 2.3., kan cookies i teorien inneholde hva som helst. Teknologien setter ikke begrensninger på annet enn mengden informasjon som kan lagres i hver cookie. Situasjoner hvor sensitive personopplysninger kan tenkes å bli behandlet, er for eksempel der en persons søkehistorie i en søkemotor behandles, eller der pasientjournaler eller strafferegister behandles på nett. De siste to vil ikke drøftes her, ettersom alle som behandler denne typen journaler på nett har lovhjemmel til å gjøre dette – henholdsvis i helseregisterloven og strafferegistreringsloven. Disse opplysningene er utilgjengelige for andre enn de autoriserte behandlingsansvarlige,[69] og det er også streng taushetsplikt for behandlingsansvarlige etter begge lover.[70]

Problemer kan oppstå når en behandlingsansvarlig setter flere cookies, og hver enkelt inneholder forskjellige opplysninger om søkehistorie, lokalisering, aldersgruppe eller lignende. Ettersom definisjonen av sensitive personopplysninger er en presisering av

---

[68] Johansen (2001) s. 78.
[69] Helseregisterloven § 13, strafferegistreringsloven § 2.
[70] Helseregisterloven § 15, strafferegistreringsloven § 8.

personopplysningsdefinisjonen, må kravet til tilknytning antas å være likt for de to definisjonene. Også indirekte tilknytning faller dermed innenfor definisjonen. Dersom en behandlingsansvarlig har tilgang til et samlet sett med opplysninger som kan knyttes til en enkeltperson, og disse opplysningene gir antydning om opplysninger som nevnt i § 2 (8), må opplysningene dermed i samlet form kunne anses å være sensitive.[71] Som eksempel kan nevnes en person som på sin private laptop søker informasjon om HIV-smitte og behandling av HIV/AIDS, eller en som registrerer seg som medlem av et ekstremistisk religiøst eller politisk nettforum. Opplysninger om denne personens søkehistorie kan implisitt si noe om hans eller hennes helsemessige forhold, religiøse overbevisning eller politiske standpunkt, uten at personen på noen måte har oppgitt informasjonen frivillig. Disse opplysningene bør anses som svært sensitive.

Ettersom det i de fleste tilfeller hvor cookies lagres ikke er snakk om denne typen opplysninger, kan man ikke kategorisk si at cookies er sensitive personopplysninger etter personopplysningsloven § 2 (8). Likevel må man konkludere med at cookies *kan* være sensitive personopplysninger, og at man må vurdere dette i hvert enkelt behandlingstilfelle. Schartum og Bygrave beskriver et system for kategorisering av personopplysninger i de to kategoriene opplysningstype og opplysningsverdi.[72] Ved å utelukke behandling av opplysninger som tilhører bestemte kategorier, kan den behandlingsansvarlige oppfylle sin informasjonsplikt og samtidig unngå behandling av sensitive personopplysninger. Mange aktører som lagrer cookies løser dette spørsmålet ved at de eksplisitt garanterer i sin *personvernspolicy*[73] at de ikke behandler noen kategorier av sensitive personopplysninger. For eksempel er det i et rammeverk som er utarbeidet for den europeiske reklameindustrien bestemmelser om at slike personopplysninger ikke skal behandles.[74] Dette rammeverket vil jeg beskrive nærmere i kapittel 3.3.

---

[71] Article 29 Data Protection Working Party: WP 136 (2007) s. 13.
[72] Schartum (2011) s.127 flg.
[73] En personvernpolicy er en erklæring fra en part om hvilke typer informasjon den samler inn fra brukeren, og hvordan den samles, behandles, og deles.
[74] EASA [1](2011).

3 Cookiedirektivet

3.1 Presentasjon av direktivet

Det såkalte *cookiedirektivet* er et endringstillegg til blant annet Direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor (kommunikasjonsverndirektivet). Cookiedirektivet ble vedtatt av Europaparlamentet og Rådet i EU den 25. November 2009. Direktivet er en del av den store reformen av EUs regelverk om elektronisk kommunikasjon som har pågått de siste femten årene. Endringene i kommunikasjonsverndirektivet er begrunnet med et behov for å styrke personvernet og informasjonssikkerheten ved bruk av elektroniske kommunikasjonsnett- og tjenester, samt et ønske om å bygge og opprettholde tilliten brukerne har til ny teknologi.[75] De kan kanskje ses på som et resultat av den raske utviklingen av internett som kommunikasjonsform og næringskilde. Bruken av internett øker både på forbrukersiden og næringssiden, men svært mange brukere har likevel ikke noen økt kunnskap eller forståelse for hvordan internett og programvare fungerer. Dette gjør kanskje at man i dag ser et større behov for å beskytte personvernet på internett enn man så for bare ti år siden. Med kommunikasjonsverndirektivet ønsket man å fremme brukernes rett til personvern og deres rett til autonomi og selvbestemmelse. Dette følger av fortalene til både det opprinnelige kommunikasjonsverndirektivet og tillegget av 2009, hvor det blant annet er uttalt at man ønsket å verne om brukernes rett til selv å bestemme over egen kommunikasjon, eget kommunikasjonsutstyr, og opplysninger om seg selv.[76] I tillegg til de mer overordnet prinsipielle hensynene bak cookiedirektivet, spiller også hensynet til brukernes informasjonssikkerhet inn, og særlig vernet mot angrep rettet mot brukerne som nevnt i kapittel 2.2.3.[77]

Det er med cookiedirektivet gjort flere endringer i kommunikasjonsverndirektivet. Blant disse er endringer i varslingsplikten til tilbydere av elektroniske kommunikasjonstjenester

---

[75] Europaportalen (2007).
[76] Direktiv 2009/136/EF, fortale nummer 23 flg.
[77] Direktiv 2009/136/EF, fortale nummer 26.

om sikkerhetsbrudd og en utvidelse av vernet mot "spam". Som jeg skal se nærmere på her, er det også innført strengere krav til informasjon og innhenting av samtykke til lagring av cookies. Sistnevnte endring medfører strengere krav til de behandlingsansvarlige, de som lagrer cookies i brukernes utstyr. For det første må behandlingsansvarlige etter direktivet informere brukerne på en måte som er tydeligere og mer grundig enn før. For det andre stilles det i direktivet krav til at brukeren på forhånd må ha gitt sitt samtykke til at cookies kan lagres hos dem, og dette samtykket må være aktivt og uttrykkelig. Hva som ligger i de nye kravene vil jeg se nærmere på i de følgende kapitlene.

3.2 Reaksjoner fra den europeiske reklameindustrien

Direktivet har ført til forsøk fra den europeiske reklameindustrien på å tilpasse seg de nye cookiereglene. Blant annet har European Advertising Standards Alliance (EASA)[78] og Internet Advertising Bureau Europe (IAB Europe)[79] den 14. april 2011 publisert et felles rammeverk for EU-landene som de ønsker at industrien for atferdsrettet reklame skal rette seg etter.[80] I rammeverket er det lagt frem noen prinsipper som alle aktører innenfor nettbasert atferdsrettet reklame må forholde seg til. Blant annet stilles det krav om at brukerne skal informeres om behandling av personopplysninger på en klar og forståelig måte.[81] Denne informasjonen kan gjøres tilgjengelig via et ikon på nettsiden hvor opplysninger samles fra. Videre skal det være valgfritt for brukeren om opplysninger skal behandles.[82] Rammeverket krever imidlertid kun uttrykkelig forhåndssamtykke i tilfeller hvor det brukes behandlingsteknologier som muliggjør behandling av opplysninger over flere domener. Det kreves også at de behandlingsansvarlige skal sørge for informasjonssikkerhet ved å opprettholde rutiner for sikker lagring og behandling av opplysninger, og i tillegg kun å lagre opplysningene så lenge som det er absolutt

---

78 http://www.easa-alliance.org/.
79 http://www.iabeurope.eu/.
80 EASA (2011) [1].
81 Id. s. 21.
82 Id. s. 22.

nødvendig.[83] Rammeverket har fått bred støtte fra reklamenettverk, annonsører og media, og EASA har også forpliktet seg overfor EU-kommisjonen til at minst 70% av medlemmene skal ha implementert de nye retningslinjene innen et år, altså innen april 2012.[84]

Rammeverket som er utformet av EASA og IAB Europe ble imidlertid møtt med sterk kritikk fra Artikkel 29-arbeidsgruppen. I et brev av 3. august 2011 uttrykte arbeidsgruppen sine innsigelser mot løsningene reklamebransjen har gått inn for.[85] For det første mente de at "opt ut"-løsningen som reklamebransjen har tatt utgangspunkt i, ikke er tilstrekkelig. EU-reglene krever eksplisitt samtykke avgitt forut for behandlingen. Løsningen i rammeverket er videre at det kreves på forhånd avgitt samtykke kun for spesielle typer behandling, noe som etter arbeidsgruppens mening ikke kan tillates. Arbeidsgruppen hevdet at brukeren alltid må ha muligheten til å tillate behandling av opplysninger til de tredjepartene han eller hun måtte ønske. Løsningen med kun å informere om tredjeparters behandling hvor denne er av en annen type enn førstepartens kunne ifølge gruppen ikke tillates. Arbeidsgruppen kommenterte også at innføringen av et ikon brukt som en grafisk advarsel om at cookies lagres, ikke bør tillates. Et slikt ikon vil, ifølge arbeidsgruppen, ikke utgjøre en tilstrekkelig klar og tydelig informasjon om lagring av cookies, i alle fall ikke så lenge dette ikonet ikke er gjenkjennelig for brukerne. Arbeidsgruppen mente også at graden av tilgjengelighet som reklamebransjen tok utgangspunkt i, ikke var tilstrekkelig. Det holder ikke at brukeren skal kunne finne relevant informasjon ved å benytte seg av forskjellige linker (og dyplinker). Den informasjonen som er avgjørende for brukerens valg må være direkte tilgjengelig og synlig på det aktuelle nettstedet.

Det er tydelig at Artikkel 29-arbeidsgruppen ikke er fornøyd med reklamebransjens tolkning og planlagte praktisering av cookiedirektivet. Det må her presiseres, som nevnt i kapittel 1.3., at arbeidsgruppens uttalelser ikke har noen direkte rettskildemessig betydning

---

[83] Id. s. 23.
[84] Id. s. 3.
[85] Article 29 Data Protection Working Party: Letter (2011).

for medlemslandene. Reklamebransjen har dermed ikke noen plikt til å følge retningslinjene som arbeidsgruppen angir. Det er likevel medlemmer fra de forskjellige landenes datatilsynsmyndigheter som sitter i arbeidsgruppen. Det er som regel disse som fører tilsyn og kontroll med bestemmelsene i direktivet på nasjonalt nivå. Sannsynligheten er stor for at mange av disse medlemmene viderefører de synspunkter som kommer frem i gruppen når det gjelder kravene de stiller til praktiseringen i sine egne land. Uansett hvordan datatilsynsmyndighetene stiller seg i forhold til cookiereglene, kan det likevel ta lang tid før direktivets regler fullt ut praktiseres av reklamebransjen. Man kan kanskje argumentere for at så lenge reklamebransjen ikke er med på å sette direktivet ut i livet, og brudd på direktivet heller ikke håndheves særlig strengt, vil ikke cookiedirektivet få noen praktisk betydning.

3.3 Samtykkekravet i Cookiedirektivet

Samtykke fra brukeren er det mest omdiskuterte grunnlaget for behandling av personopplysninger ved bruk av cookies. Jeg vil drøfte samtykkereglene i forbindelse med behandling av personopplysninger inngående i kapittel 4. For der å kunne drøfte personopplysningslovens samtykkekrav i lys av de nye cookiereglene, er det først nødvendig å se på kravet til samtykke slik det er lagt til grunn i cookiedirektivet.

Cookiedirektivet er et tillegg til, og således også en forlengelse av, kommunikasjonsverndirektivet og dets tilleggsbestemmelser. Direktivet gjør seg dermed, likedan som kommunikasjonsverndirektivet, gjeldende for behandling av personopplysninger i sammenheng med tilbud om offentlig tilgjengelige elektroniske kommunikasjonstjenester i offentlige kommunikasjonsnettverk.
Hva angår samtykkedefinisjonen, henviser imidlertid kommunikasjonsverndirektivet i artikkel 2.2 (f) til personverndirektivet. Det følger videre av kommunikasjonsverndirektivets fortale nummer 17 at samtykkebegrepet her skal tillegges den samme betydning som i personverndirektivet. I personverndirektivet artikkel 2(h) er samtykke definert som følger:

> " 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Denne definisjonen ligger nært opp mot samtykkedefinisjonen i personopplysningsloven. Jeg vil drøfte de enkelte vilkårene inngående i kapittel 4 om definisjonen av samtykke til behandling av personopplysninger i norsk rett. Cookiedirektivet gir ikke noen egen spesifikk definisjon av samtykke, men henviser i fortalens nummer 17 til kommunikasjonsverndirektivet og personverndirektivet for definisjonene som finnes der. I cookiedirektivet artikkel 5 (3), som erstatter samme artikkel i kommunikasjonsverndirektivet, er det likevel uttrykt at det må stilles krav til at brukeren forut for behandlingen har fått klar og forståelig informasjon om behandlingen:

> "(…) the subscriber or user has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing."

Selv om cookiedirektivets samtykkedefinisjon bygger på den i personverndirektivet, er kommunikasjonsverndirektivet for *lex specialis* å anse i forhold til personverndirektivet.[86] Spesielle kriterier i førstnevnte må følgelig tas i betraktning når man for eksempel vurderer spørsmål om lagring av cookies. Selv om samtykke ikke er gitt, åpner reglene i cookiedirektivet for at visse typer behandling likevel er tillatt, som lagring av tekniske, kommunikasjonsmessig nødvendige eller servicemessige grunner. Jeg kommer tilbake til slike unntak i kapittel 4, hvor jeg drøfter samtykkebegrepet i norsk rett.

Det er en stor grad av samsvar når det gjelder utformingen av samtykkekravet i de forskjellige EU-direktivene som omhandler personvernet, og de bygger også på de samme

---

[86] Article 29 Data Protection Working Party: WP 187 (2011) s. 28.

prinsippene. Også i norsk rett bygger utformingen i stor grad på den som følger av direktivene, noe jeg vil drøfte i kapittel 4. Selv om EU-direktivene presenterer en nokså samlet og unison definisjon av samtykkebegrepet, varierer imidlertid tolkningen av samtykkebegrepet mellom de forskjellige EU-landene. De største forskjellene ligger i hvordan vilkårene for å behandle personopplysninger tolkes.

3.4 Implementering av samtykkekravet i noen medlemsland

3.4.1 Introduksjon

Implementeringen av cookiedirektivet i de forskjellige EU-landene har gått sakte, og er preget av stor variasjon mellom de forskjellige landene. Dette har nok sitt utspring i at EU-kommisjonen i forholdsvis stor grad åpnet for at landene kunne implementere personverndirektivet slik det passet deres rettssystem og sammenhengen med den øvrige lovgivning best. Dette følger blant annet av personverndirektivets fortale nummer 23. I cookiedirektivet er det videre foreslått at medlemslandene oppretter egne nasjonale tilsynsmyndigheter som skal ha ansvaret for å kontrollere og håndheve reglene. Dette følger av direktivets artikkel 15 (a) og fortalens nummer 69. Tilsynsmyndighetene må ha myndighet til å etterforske og følge opp saker vedrørende regelbrudd, og de må ha myndighet til å sanksjonere disse bruddene.

Jeg vil i det følgende se nærmere på implementeringsprosessene i noen utvalgte EU-land. Det er forskjellige grunner til at jeg har valgt å fokusere på akkurat disse landene. Danmark valgte jeg fordi det danske rettssystemet ligger tett opp mot det norske, og fordi Danmark var et av landene som var tidligst ute med å sette i gang implementeringsprosessen. Storbritannia og Frankrike valgte jeg fordi de er store og viktige land i EU, både økonomisk og politisk. Nederland ble valgt på grunn av at de er trukket frem som det landet med den mest radikale tolkningen av cookiereglene, ettersom den stiller strenge krav til samtykke. Jeg vil gå gjennom de forskjellige landenes prosesser, og til slutt forsøke å trekke noen linjer mot det norske rettssystemet.

3.4.2 Danmark

Danmark var et av de første medlemslandene som foreslo lov- og forskriftsendringer i tråd med cookiedirektivet. Våren 2011 ble et utkast til en ny forskrift sendt til høring av Det danske vitenskapsdepartementet med høringsfrist den 1. april 2011.[87] Formålet med den nye forskriften var blant annet å sørge for at brukerne får bedre informasjon om lagring av opplysninger, for eksempel i form av cookies, på deres kommunikasjonsutstyr.[88] Utkastet innebærer et krav om at brukeren må ha gitt et klart og informert samtykke for at cookies skal kunne lagres på hans eller hennes brukerutstyr. Samtykket defineres i utkastets § 3 nr. 2 som "enhver frivillig, specifik og informeret viljestilkendtgivelse", noe som tilsvarer den norske definisjonen i personopplysningsloven § 2 nr.7. Til informasjonsplikten stilles det i utkastets § 3 nr. 3 krav om at informasjonen skal fremstå i et "klart, præcist og letforståeligt sprog", og at "formålet med lagringen af eller adganger til oplysninger" må komme klart frem. Det er imidlertid ikke sagt noe i forslaget om hvorvidt samtykket må være avgitt forut for behandling av, eller adgang til, cookies. IT- og Telestyrelsen (den danske datatilsynsmyndigheten) deler ikke EU-kommisjonens syn på at det bør stilles krav til forhåndssamtykke, og har bevisst valgt å utelukke dette kravet fra forslaget.[89] Dette betyr at forhåndsdefinerte innstillinger i nettleseren som godtar cookies, fortsatt vil kunne være mulig etter forslaget.

Etter å ha mottatt høringsuttalelser i saken bestemte imidlertid Det danske vitenskapsdepartementet seg i mai 2011 for å utsette implementeringen av cookiedirektivet. Begrunnelsen de oppga var at EU-reglenes krav om samtykke måtte avklares nærmere før de kunne implementere direktivet. Kontorsjefen i IT- og Telestyrelsen, Kresten Bay, sa i et intervju på nettsidene til IT- og Telestyrelsen at "Formålet med reglerne er at øge beskyttelsen af borgernes privatliv på nettet. Samtidig er det vigtigt, at onlinebranchen fortsat kan trives og skabe vækst på det digitale marked i Danmark og i Europa."[90] Man ser

---

[87] Ministeriet for Videnskab, Teknologi og Udvikling [1] (2011).
[88] Ministeriet for Videnskab, Teknologi og Udvikling [2] (2011).
[89] IT-sikkerhedskomiteen (2011).
[90] IT- og Telestyrelsen [1] (2011).

altså at hensynet til økonomisk vekst og teknologisk utvikling er vel så høyt vurdert som personvernet. Det er imidlertid ikke gitt noen indikasjoner på hvordan denne interesseavveiningen vil skje etter den nærmere avklaringen.

3.4.3 Frankrike

Den franske lovgivningen som regulerer personvernspørsmål i forbindelse med lagring av cookies, er lov nummer 78-17 av 6. januar 1978 om informatikk, filer og friheter.[91] I denne loven finner man blant annet regler om hvordan personopplysninger skal behandles, og regler om kravet til personers samtykke til slik behandling. Det er særlig artikkel 32 om forpliktelser som er pålagt den behandlingsansvarlige som er relevant for lagring og behandling av cookies. Man finner i denne bestemmelsen en implisitt definisjon av samtykkekravet i uttrykket "(…)ait exprimé, après avoir reçu cette information, son accord (…)". Samtykket må være *uttrykt* etter at brukeren har mottatt *informasjon*. Kravet til informasjon i bestemmelsen tilsvarer i all hovedsak personverndirektivets krav i artikkel 6 og 7, som nevnt ovenfor i kapittel 3.4.

Implementeringen av cookiedirektivet ble blant annet gjennomført ved en endringsforskrift av 24. august 2011,[92] som er en del av "Paquet Télécom" (telekompakken). Denne forskriften gjør blant annet endringer i loven av 1978. I forskriftens tredje kapittel, artikkel 37, er det vedtatt endringer i den ovenfor nevnte artikkel 32. Etter den reviderte artikkel 32, nr. II, kan tilgang til eller behandling av personopplysninger kun finne sted dersom den berørte personen uttrykkelig har gitt sitt informerte samtykke til dette. Slikt samtykke kan likevel anses som gitt gjennom personens innstillinger for oppkobling til internett. Dette betyr at blant annet innstillinger i den berørte personens nettleser kan godtas som et samtykke til lagring av cookies. Personen må imidlertid ha samtykket til innstillingene på forhånd. I praksis godtas dermed ikke samtykke gjennom innstillinger i nettleser uten at de forhåndsdefinerte innstillingene i utgangspunktet nekter lagring av cookies.

---

[91] Loi Informatique et Libertés. Lov nummer 78-17 av 6. januar (1978).
[92] Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques.

La Commission nationale de l'informatique et des libertés (CNIL – det franske datatilsynet)[93] ga 9. juni 2011 sin høringsuttalelse i forbindelse med forskriften som ble vedtatt 24. august 2011. Høringsuttalelsene publiseres dessverre ikke, men på nettsidene sine har CNIL gitt uttrykk for sin misnøye med samtykkebegrepet som er lagt til grunn i forskriften. De hevder at innstillinger i brukerens nettleser ikke under noen omstendigheter kan anses som brukerens samtykke til lagring av cookies. Kravet til informert samtykke innebærer ifølge CNIL at brukeren skal informeres om det enkelte formålet med enhver cookie som settes på hans eller hennes kommunikasjonsutstyr. Dette er ikke mulig ved et generelt samtykke gitt gjennom nettleserinnstillinger, da informasjon om det enkelte formål ikke fremkommer her. [94]

Selv om der fortsatt er uenighet rundt enkelte spørsmål, har den franske implementeringen i alle fall blitt gjennomført, og kravet til samtykke synes å tolkes forholdsvis strengt, sammenliknet med situasjonen i Danmark.

3.4.4 Storbritannia

I Storbritannia ble reglene angående bruk av cookies endret den 26. mai 2011 gjennom "The Privacy and Electronic Communications Regulations 2003" (PECR), en dag etter implementeringsfristen satt av EU-kommisjonen.[95] Artikkel 6 nr. 2 i denne loven setter betingelser på brukersiden for at databehandleren skal kunne lagre personopplysninger. Før lovendringen var betingelsene at brukeren skulle ha hatt tilgang til forståelig og fullstendig informasjon angående formålene med lagringen, og at brukeren skulle vært gitt muligheten til å motsette seg lagringen. Denne sistnevnte muligheten til å motsette seg lagring er nå endret til et krav om at brukeren skal ha gitt sitt samtykke forut for lagringen.

Bestemmelsens nr. 3 og 3A utdyper videre hva som skal legges i samtykkebegrepet. For det første presiseres det i nummer 3 at dersom brukeren besøker en nettside mer enn én

---

[93] www.cnil.fr.
[94] CNIL (2011).
[95] The Privacy and Electronic Communications No. 1208 (2011).

gang, er samtykke ved første besøk tilstrekkelig gjeldende samtykke også for de eventuelle påfølgende besøk.[96] Videre følger det av nr. 3A at samtykke gjennom innstillinger i brukerens nettleser eller ved bruk av applikasjoner eller programmer vil kunne godtas som samtykke til lagring av cookies.[97]

Lovteksten i PECR artikkel 6 nr. 2 er svært vag, og krever kun brukerens samtykke uten videre utdyping av hva som legges i dette. Videre gir artikkelens nummer 3A grunn til å anta at nettleserinnstillinger i alle fall i enkelte tilfeller vil kunne godkjennes som et brukersamtykke. Det er ikke gitt noen anvisning på om forhåndsdefinerte innstillinger vil godtas etter bestemmelsen. De britiske lovgiverne har altså tatt et nokså næringsvennlig standpunkt til lagring av cookies. I sin anbefaling til virksomheter angående lagring av cookies foreslår likevel The Information Commissioner's Office (ICO – det britiske datatilsynet) at virksomheter som setter cookies innhenter brukernes samtykke på andre måter enn ved forhåndsdefinerte innstillinger i nettleseren.[98] Samtykke kan for eksempel innhentes gjennom "pop up"-vinduer, informasjon i brukervilkårene, valg i nettsideinnstillinger eller valg av særlige tjenester på en nettside. Også ICO ser imidlertid ut til å vektlegge næringslivets interesser. Informasjonskommissæren, som skal håndheve reglene, har innført en 12 måneder lang overgangsperiode fra mai 2011 til mai 2012 som gir virksomheter og organisasjoner tid til å finne praktiske løsninger for hvordan de vil innhente samtykke til lagring av cookies.[99] Regelverket vil altså ikke i praksis håndheves før i mai 2012. I tillegg uttaler den britiske informasjonskommissæren at håndhevingen av cookiereglene også etter mai 2012 vil være gjenstand for en skjønnsmessig vurdering.[100] Konsekvensen for brukernes personvern ved regelbrudd vil veies opp mot virksomheters tekniske behov.[101]

---

[96] Id.
[97] Id.
[98] Information Commissioner's Office [1](2011) s. 5.
[99] Information Commissioner's Office [2](2011).
[100] Id. s. 6.
[101] Id. s. 6.

3.4.5 Nederland

I november 2010 introduserte Det nederlandske departementet for økonomi, landbruk og innovasjon en lov som skulle fungere som et tillegg til Telecommunicatiewet (den nederlandske loven om telekommunikasjon).[102] Den foreslåtte loven stilte strengere krav til samtykke og informasjonsforpliktelser rundt lagring av cookies. I det endelige utkastet stilles det krav om at brukeren må ha gitt sitt *utvetydige samtykke* forut for lagring. Dette ble kritisert av næringslivsaktørene, som mente at man ikke kunne stille et samtykkekrav som i praksis innebar at det måtte samtykkes til hver enkelte cookie som lagres i en brukers elektroniske utstyr. Det nederlandske datatilsynet, Ministeren for økonomi, landbruk og innovasjon, samt initiativtakerne til den nye loven har imidlertid alle gitt uttrykk for at det ikke er noe i veien for at samtykke gis gjennom innstillinger i nettleser.[103] Dette forutsetter imidlertid at de nåværende nettleserne endre på sine forhåndsdefinerte innstillinger. Dette utgjør i praksis en stor endring, særlig ettersom loven vil komme til å kreve utvetydig samtykke fra brukerne, noe som innebærer at det mest sannsynlig vil kreves samtykke til nettleserinnstillinger i form av "opt-inn", og ikke "opt-ut". Det er imidlertid uttalt i forarbeidene til lovforslaget at det ikke er meningen at databehandlere må innhente samtykke for hver eneste cookie som lagres – samtykke kan innhentes samlet for en gruppe av cookies.

Selv om den foreslåtte nederlandske loven synes å stille strengere krav til samtykke enn mange andre EU-land, er det likevel usikkert hvordan den nye loven vil komme til å håndheves. Det nederlandske post- og teletilsynet, OPTA,[104] som blant annet er ansvarlig for håndheving av nederlandsk regelverk på området for telekommunikasjon, har hittil valgt å håndheve cookieregler kun når det gjelder skadelig "spyware". Det er dermed usikkert om tilsynet kommer til å håndheve reglene for lagring av "vanlige" cookies. Den

---

[102] Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie.
[103] Simons (2011).
[104] http://www.opta.nl/en/.

foreslåtte lovendringen er i november 2011 fremlagt for det nederlandske senatet, og det er forventet at loven vil tre i kraft i januar 2012.[105]

3.5 EU-kommisjonens reaksjoner på (manglende) implementering

Selv om det kan diskuteres om de har implementert direktivene i tilstrekkelig grad, hadde både Storbritannia og Danmark startet implementeringen av regler om lagring av cookies våren 2011. I august 2011 gjennomførte Frankrike implementeringen. Det var imidlertid bare 7 av 27 land som hadde startet implementeringsprosessen for direktivene 19. juli 2011.[106] Denne datoen sendte EU-kommisjonen derfor ut offisielle brev til 20 av de 27 medlemsstatene hvor de ba om informasjon vedrørende implementeringsprosessen av tilleggene til Kommunikasjonsverndirektivet, deriblant Cookiedirektivet.[107] Disse 20 landene hadde ikke enda startet implementeringen av direktivet. Brevene innebar formelle varsler som startet direktivbruddsprosedyrer.

Etter dette har flere av medlemslandene fått fortgang i sine implementeringsprosesser. Da brevene ble sendt ut, var det 7 land som hadde startet prosessen med å implementere direktivene (Danmark, Estland, Finland, Irland, Malta, Sverige og Storbritannia).[108] I november 2011 er det 18 land som har startet implementeringsprosessen.[109] Det er imidlertid i varierende grad gjort store praktiske endringer i de enkelte landenes lovverk som berører lagring av cookies . I enkelte land, som for eksempel Storbritannia, har ulike offentlige tilsyn i tillegg gått ut og sagt at håndhevingen av direktivet i en overgangsperiode ikke vil være særlig streng.[110] Det er også publisert flere presseartikler hvor det rapporteres om at også EU-kommisjonen har signalisert at direktivet ikke trenger å tolkes for strengt. Uten at man har fått noen bekreftende eller avkreftende kommentarer fra

---

105 Simons (2011).
106 EU-kommisjonen (2011).
107 Id.
108 Id.
109 EUR-LEX [2](2011).
110 Id.

Kommisjonen selv, har det i pressen versert et internt brev fra EU-kommissær Neelie Kroes som er ment å skulle veilede medlemsstatene om hvordan direktivet bør implementeres og tolkes. Det sies visstnok i brevet at samtykke i form av en "opt-inn"-løsning ikke er et absolutt krav.[111] Dette strider mot oppfatningen av regelendringene slik norske media har presentert saken, noe jeg vil komme tilbake til i kapittel 5.3.

Hittil har det altså kommet blandede signaler fra både EU-kommisjonen og de nasjonale myndighetenes lovgivningsorganer når det gjelder tolkningen og håndhevingen av cookiedirektivet og nasjonalt implementert lovgivning. Det kan spekuleres i om ikke dette kan ha bidratt til den langvarige implementeringsprosessen i mange av medlemslandene. Det er likevel problematikken rundt samtykkekravet som ser ut til å være grunnen til de største implementeringsproblemene – og særlig forholdet til innstillinger i nettleser. Dette vil jeg drøfte mer inngående i kapittel 4 og 5, hvor cookiedirektivets bestemmelser vurderes i forhold til norsk rett.

4 Krav om samtykke til å behandle personopplysninger i norsk rett

4.1 Introduksjon

Jeg vil i det følgende se nærmere på hva som ligger i begrepet samtykke til behandling av personopplysninger i norsk rett, og hva hovedvilkårene for slikt samtykke innebærer. Jeg vil vurdere samtykkebegrepet konkret med tanke på samtykke til lagring av cookies, og de vilkårene som stilles i cookiedirektivet (se kapittel 3.4.) for at et slikt samtykke skal anses å være gitt. Eksempler som trekkes frem er derfor også eksempler som har relevans for denne typen behandling av personopplysninger. Jeg vil også forsøke å presentere noen av de tekniske løsningene som er foreslått i praksis og teori for å løse samtykkeproblemene ved lagring av cookies.

---

[111] Miller (2011).

Kravet om samtykke til behandling av personopplysninger er nedfelt i personopplysningsloven § 2 nr. 7, som sier at et samtykke er "en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv". Personopplysningens definisjon av samtykke er nært knyttet opp mot lovens forarbeider, hvor mange av definisjonselementene er beskrevet.[112] Forarbeidene henviser ofte til personverndirektivets bestemmelser, og det er derfor naturlig å drøfte kravet til samtykke i EU-direktivene og norsk rett noenlunde samlet. Jeg vil derfor her, i tillegg til å drøfte norsk rett, bruke eksempler fra EU-retten, både gjennom teori og bruk av praktiske eksempler.

Den enkeltes autonomi er et hovedprinsipp etter både norsk og europeisk personvernlovgivning, og samtykke er derfor et av de viktigste begrepsgrunnlagene for både EU-direktivene og den norske loven. Det er også grunnlag for behandling av personopplysninger, både i EU-retten og i norsk rett.[113] De fleste tilfeller av lagring av cookies som er problematiske i et personvernperspektiv, nemlig lagring av (varige) tredjepartscookies, krever samtykke fra brukeren. De øvrige grunnlagene for behandling av personopplysninger vil også i enkelte tilfeller gjelde for lagring og behandling av cookies. Det er imidlertid ikke knyttet like store tolkningsproblemer til disse behandlingsgrunnlagene som til samtykkekravet. I den videre drøftelsen er det derfor nødvendig å se nærmere på hva som ligger i det å samtykke til behandling av personopplysninger. De alternative grunnlagene for behandling vil bare vurderes i begrenset grad.

4.2 Generelle krav til behandling av personopplysninger

I personopplysningsloven § 11 stilles det noen generelle krav til behandling av personopplysninger. Disse kravene gjelder dermed også for samtykkebasert behandling av

---

[112] Ot.prp. nr.92 (1998-1999) s. 103.
[113] Personopplysningsloven § 8, personverndirektivet artikkel 7.

personopplysninger, og bør presenteres før samtykkekravet drøftes nærmere. For det første tillates behandling av personopplysninger kun etter lovens §§ 8 og 9. Videre stilles det krav til at opplysningene kun brukes til uttrykkelig angitte og saklig begrunnede formål, og at de ikke senere (uten samtykke) brukes til nye formål som er uforenlige med det opprinnelige. Det stilles også krav til at opplysningene som behandles er tilstrekkelige, relevante og adekvate, og at de ikke lagres lengre enn det som er nødvendig for å innfri det oppgitte formål. Dersom samfunnets interesse i at behandlingen finner sted, klart overskrider ulempene for den enkelte, skal senere behandling for historiske, statistiske eller vitenskapelige formål ikke anses uforenlig med det opprinnelige formål.

Bestemmelsen i § 11 gjennomfører personverndirektivet artikkel 6, som har en tilsvarende bestemmelse.[114] Kravene som stilles i § 11, er kumulative, og må alle oppfylles for at behandling av personopplysning etter §§ 8 og 9 skal kunne gjennomføres.[115] Det er derfor hensiktsmessig å ta hensyn til disse kravene også når man drøfter vilkårene for samtykke til behandling av personopplysninger. Særlig aktuelt for problematikken rundt lagring og behandling av cookies er kravene til informasjon om formål og innsamling/behandling av opplysninger. Disse kravene følger også av vilkårene for samtykke, og vil drøftes inngående i kapittel 4.3.2.3. om informasjonskravet.

4.3 Grunnlag for behandling av personopplysninger

4.3.1 Lov- og nødvendighetsgrunnlag

I personopplysningsloven § 8 er det oppstilt flere grunnlag for behandling som gjør seg gjeldende på lik linje med samtykke. Bestemmelsen i § 8 gjennomfører EU-direktivet artikkel 7, og stiller generelle og uttømmende vilkår for når behandling av

[114] Ot.prp. nr. 92 (1998-1999) s. 112.
[115] Johansen (2001) s. 115.

personopplysninger kan skje.[116] For at behandling skal tillates uten at samtykke fra den registrerte foreligger, må et av grunnlagene i § 8 foreligge.

Et grunnlag som kan være aktuelt for lagring og behandling av cookies, er tilfeller der det i lov er gitt adgang til behandling av personopplysninger, jamfør § 8, 1. ledd. Det må da stilles krav til at loven gir direkte hjemmel eller klart forutsetter slik behandling.[117] Det er flere eksempler på lovgivning som gir slik adgang, blant annet i helseregisterloven og strafferegisterloven. Det kan også tenkes at det under annen lovgivning som regulerer forskjellige typer registre og databaser, åpnes for lagring og behandling av cookies. Når det gjelder cookies som brukes til kommersielle formål, er det imidlertid tvilsomt om man kan basere lagring og behandling på lovhjemmel. I så fall vil dette ikke være tilfelle særlig ofte. Lov som behandlingsgrunnlag vil derfor ikke drøftes videre.

I tillegg til grunnlag i lov, følger det av personopplysningsloven § 8 (a-f) seks øvrige grunnlag som gir adgang til behandling. Disse utgjør de såkalte *nødvendighetsgrunnlagene* for behandling av personopplysninger. Hvis man skal sammenholde disse med den type behandling som drøftes her, nemlig lagring og behandling av cookies til kommersielle formål, ser man at få eller ingen av de nevnte unntakene gjør seg gjeldende. Der er sjelden rettslig eller kontraktmessig nødvendig å sette cookies for å følge med på brukernes internettaktivitet, jamfør § 8 (a-b). De få tilfeller hvor det finnes lovhjemmel for slik behandling av personopplysninger uten samtykke, kan være saker hvor det er behov for informasjon i etterforskningsøyemed og hvor behandling er tillatt i medhold av datalagringsdirektivet. Her har behandlingen helt andre formål enn de kommersielle. Det kan videre diskuteres om behandlingsansvarlige kan sies å ha en berettiget økonomisk interesse i å sette cookies, jamfør § 8 (f). Mange nettsider finansieres i dag fullt ut av annonsørene sine, og også media er i stor grad økonomisk avhengig av annonsesalg. Likevel har jeg vanskelig for å se at det ikke kan annonseres på nettsider uten at man bruker cookies og andre tekniske hjelpemidler til brukerprofilering. Det har muligens

---

[116] Ot.prp. nr. 92 (1998-1999) s. 108.
[117] Schartum (2011) s. 163.

utviklet seg et krav fra annonsører om at annonsene deres skal rettes direkte mot målgruppene, men lagringen av cookies kan neppe anses å være berettiget overfor brukerne. Dersom man veier hensynet til de enkelte næringsdrivendes økonomiske interesser opp mot hensynet til vern av personopplysninger, synes førstnevnte interesser klart mindre tungtveiende. De øvrige nødvendighetsgrunnene i § 8 vil antakelig sjelden gjøre seg gjeldende for lagring av cookies for kommersielle formål. Jeg vil derfor ikke gå nærmere inn på disse.

4.3.2 Samtykke

Samtykkebegrepet er basert på grunntanken om individers autonomi og selvbestemmelsesrett, en tanke som blant annet står sterkt innenfor avtaleretten.
De tre hovedkriteriene for samtykke er at det må være frivillig, uttrykkelig og informert.[118] Dersom et av kriteriene mangler, foreligger normalt ikke gyldig samtykke.

I forarbeidene til personopplysningsloven er det i merknaden til personopplysningsloven § 2 gjort oppmerksom på at definisjonene i bestemmelsen dels baserer seg på den gamle personregisterloven og dels på definisjonene i personverndirektivet artikkel 2.[119] Selv om utformingen av definisjonene er noe annerledes enn i direktivet, er hovedvilkårene for samtykke til behandling av personopplysninger tilsynelatende sammenfallende i norsk rett og EU-retten. Kravene til frivillighet, uttrykkelighet og informasjon er til stede i begge rettssystem. Hva disse kravene innebærer, er imidlertid ikke like åpenbart. Lovgivernes begrepsbruk er svært vag, og den åpner i stor grad for tolkning. Jeg vil derfor også trekke inn argumenter fra EU-retten og praksis i gjennomgangen av hovedvilkårene for samtykke etter personopplysningsloven § 2 nr. 7.

---

[118] Schartum (2011) s. 161.
[119] Ot.prp. nr. 92 (1998-1999) s. 101.

4.3.2.1 Kravet om frivillighet

Kravet om frivillighet er en helt fundamental del av prinsippet om individers autonomi og selvbestemmelsesrett, og er utgangspunktet for avtaleretten. Foreligger det ikke noen frivillig avgitt viljeserklæring, foreligger det heller ikke noen avtale. Dette gjenspeiler seg blant annet i ugyldighetsreglene i avtaleretten, hvor avtaler som er inngått under former for tvang, utnyttelse eller svik anses for ugyldige.[120] Det første kriteriet for samtykke etter personopplysningsloven § 2 nr.7, er at det må være *frivillig avgitt*. I dette ligger at samtykket ikke må være gitt under noen form for tvang eller i tvangslignende situasjoner, verken fra behandlingsansvarlige eller noen andre.[121] Ifølge Schartum og Bygrave innebærer kravet trolig også at det ikke skal være noen negative konsekvenser knyttet til det å ikke gi sitt samtykke.[122] Dette er en betraktning som også er gjort i forbindelse med personverndirektivet. Artikkel 29-arbeidsgruppen har med tanke på personverndirektivet artikkel 8(2)(a) uttalt:

> "(…)free consent means a voluntary decision, by an individual in possession of all of his facilities, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as 'free' (…)".[123]

Grunnen til at samtykke som er gitt under en trussel om ikke-behandling eller dårligere behandling ikke anses som et frivillig samtykke, er at man her i realiteten står overfor en tvangssituasjon. Et spørsmål man imidlertid kan stille, er om det er alvoret i situasjonen som vektlegges – behovet for medisinsk behandling er primært, og i mange tilfeller livsnødvendig – eller en mer generell idé om at ønsket om å opprettholde eget personvern ikke skal gå ut over den behandling man normalt ville fått. Dersom det er hensynet til generelt god behandling som vektlegges, kan man kanskje hevde at også negative tekniske

---

[120] Avtaleloven kapittel 3.
[121] Ot. Prp. Nr.92 (1998-1999) s. 104.
[122] Schartum (2011) s. 161.
[123] Article 29 Data Protection Working Party: WP 131 (2007) s. 8.

konsekvenser for brukere av hvilke som helst slags internettbaserte tjenester må føre til en manglende reell frivillighet. Videre kan man kanskje innfortolke "technical coercion" i uttrykket "social, financial, psychological or other coercion". Samtykke til lagring av cookies basert på trusselen om dårligere teknisk funksjonalitet, ikke-fungerende eller dårligere fungerende nettsider og tilbud ved manglende samtykke, kan i så fall ikke anses som frivillig.

Personvernnemnda har i en klagesak av 2003 uttalt seg om kravet til frivillighet, og anser det slik at "(…) når samtykke stilles som betingelse for å få et gode av betydning for den registrerte, vil som hovedregel samtykket ikke kunne anses å være avgitt frivillig." [124] Saken gjaldt Kredittnetts krav om samtykke til registrering i deres sentrale låneregister ved eventuelle innvilgelser av lån. Nemnda mente at det i denne saken var åpenbart at samtykke i denne situasjonen ikke kunne anses å være avgitt frivillig, ettersom registrering i låneregisteret her i praksis ble stilt som vilkår for at søknader i det hele tatt skulle behandles. Nemndas uttalelse kan tale for at nettsider ikke kan gjøre tilgang til full teknisk funksjonalitet og tjenester betinget av samtykke til lagring av cookies. Mange nettsider legger inn nettopp denne typen ansvarsfraskrivelser i sin personvernpolicy. Her må man imidlertid skille mellom ulike typer cookies. Noen cookies er helt nødvendige for å sikre funksjonalitet og sikkerhet på nettsted, mens andre settes utelukkende for å muliggjøre brukerprofilering og personlig rettet reklame. Midlertidige førstepartscookies innehar ofte slike nødvendige tekniske funksjoner. Lagring av denne typen cookie vil normalt ikke innebære negative konsekvenser for brukerens personvern. De eventuelle negative følgene av slik lagring er i så fall nødvendige, og må vike for hensynet til brukerens selvbestemmelsesrett. Nettsted som for eksempel gjør full funksjonalitet betinget av at tredjeparter kan sette varige cookies hos brukeren, har derimot neppe tilstrekkelige tekniske begrunnelser for dette. Samtykke under slike betingelser kan ikke anses som frivillig avgitt.

[124] PVN-2003-01 Klagesak.

4.3.2.2 Kravet om uttrykkelighet

Et neste vilkår for samtykke er at det skal være *uttrykkelig* avgitt. Dette innebærer for det første at det må foreligge en erklæring, jf. Personopplysningsloven § 2 nr. 7. For det andre må erklæringen være utvetydig.[125]

Kravet til at det må foreligge en *erklæring* innebærer at samtykket må være gitt i fysisk form. Dette er klart uttrykt i forarbeidene til personopplysningsloven, som understreker at verken passivt eller stilltiende samtykke, ei heller konkludent atferd er tilstrekkelig uttrykkelig.[126] Det er utover dette åpnet for at alle typer viljeserklæringer kan falle inn under formkravet til et samtykke. En vid formforståelse legges imidlertid til grunn, hvor også muntlige og elektroniske samtykker kan falle inn under samtykkebegrepet.[127] Dette følger også av forarbeidene, hvor det presiseres at samtykke kan gis skriftlig eller muntlig, så vel som elektronisk.[128] Bevisbyrden for at det er avgitt samtykke ligger på behandlingsansvarlige.[129] Dette fører til at det i praksis stort sett vil måtte avgis skriftlig eller elektronisk samtykke, ettersom muntlige samtykker er mye vanskeligere å bevise. Muntlige samtykker er uansett lite aktuelle når det gjelder lagring av cookies, ettersom samtykke i disse tilfellene avgis elektronisk. Det kan videre drøftes hvorvidt samtykke til lagring av cookies gjennom forhåndsdefinerte innstillinger i nettleser bør anses som en erklæring. Slike samtykker kan kanskje defineres som konkludente. I norsk rett er passivt eller konkludent samtykke ikke ansett å være tilstrekkelig etter personopplysningsloven. Dette er uttalt både i forarbeidene og i rettspraksis, blant annet i et vedtak truffet av Personvernnemnda i 2010, hvor det hevdes at "(d)ersom et samtykke skal være reelt må den som samtykker være informert og ta et aktivt valg".[130] En erklæring må altså antas å innebære et aktivt valg, noe man som bruker kanskje ikke kan anses å ha tatt ved å unnlate

---

[125] Ot.prp. nr. 92 (1998-1999) s. 103
[126] Ot.prp. nr. 92 (1998-1999) s. 102 flg.
[127] Article 29 Data Protection Working Part: WP 187 (2011) s. 11.
[128] Ot. Prp. Nr.92 (1998-1999) s.103.
[129] Id.
[130] PVN-2010-09 Ung i Norden.

å endre på nettleserinnstillingene sine. Jeg vil drøfte dette og andre spørsmål om innstillinger i nettlesere i kapittel 4.5.

Det følger av personopplysningslovens forarbeider at det *klart og utvetydig* må fremgå at det samtykkes, og også hva og hvem samtykket gjelder.[131] Det må være helt klart hvilken behandling samtykket refererer seg til, og hvilke formål og konsekvenser det har. Alle de forskjellige typene personopplysninger som kan behandles og formålene med disse må dermed fremgå i forbindelse med samtykket. Kravet til utvetydighet er ikke uttrykkelig formulert i loven, men presiseres i forarbeidene. Det er også uttrykkelig formulert i personverndirektivet artikkel 7 (a), som krever at "the data subject has unambiguously given his consent". Det er imidlertid knyttet en viss usikkerhet til kravet om utvetydighet. Mangelen på klare retningslinjer kan kanskje gjøre det vanskelig å håndheve. Resultatet blir at kravet må tolkes objektivt for det enkelte tilfelle, og dette kan føre til at mange av aktørene som behandler personopplysninger velger å tolke kravet i vid forstand og innlemme også det passive eller konkludente samtykket i definisjonen. Dette kan føre til det som i realiteten er tvetydige og uklare samtykker, noe som er et personvernmessig og rettssikkerhetsmessig problem. Dette er noe Artikkel 29-arbeidsgruppen også problematiserer. I sin uttalelse om samtykkedefinisjonen sier de at "In practice, the ambiguity of a passive response will make it difficult to fulfil the requirements of the Directive".[132]

Man kan kanskje hevde at en bruker som selv har lastet ned eller kjøpt et nettleserprogram, allerede i denne handlingen må sies å ha gitt et aktivt og utvetydig samtykke til den behandling som følger av nettleserens forhåndsdefinerte innstillinger. Det samme kan hevdes for brukere som registrerer kundekonti hos ehandelsportaler som eBay og Amazon. Særlig i de sistnevnte tilfeller vil man kunne argumentere for at lagring og behandling av cookies til kommersielle formål er noe brukeren har samtykket til. Det er jo nettopp kommersiell virksomhet som er kjernen i disse portalenes formål. Et problem med denne

---

[131] Ot.prp. nr. 92 (1998-1999) s. 104
[132] Article 29 Data Protection Working Party: WP 187 (2011) s. 12.

argumentasjonen er at man i tillegg må stille spørsmål ved om brukeren har tilstrekkelig kunnskap til å forstå hva de forhåndsdefinerte innstillingene innebærer. Dette fører oss over i det tredje kravet til samtykke: informasjonskravet.

4.3.2.3 Informasjonskravet

Det er kravet om informert samtykke som nok byr på de største tolkningsproblemene i praksis. Hvilke krav skal man stille til informasjonens innhold, dens klarhet, og dens omfang? For mye informasjon kan føre til motsatt resultat av det som er ønskelig, nemlig at brukeren føler avmakt og unngår å sette seg inn i informasjonen som gis. På den annen side kan for lite eller for vag informasjon føre til at brukeren overhodet ikke forstår omfanget av behandlingen han eller hun samtykker til. Begge disse situasjonene kan føre til utilstrekkelig informerte samtykker.

Informasjonskravet følger av personopplysningsloven § 2 nr.7, som sier at samtykket skal være "en frivillig, uttrykkelig og *informert* erklæring". Hva som ligger i kravet er presisert i § 19. Her stilles det krav om at den behandlingsansvalige uoppfordret skal informere den registrerte om:

> "a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
> b) formålet med behandlingen,
> c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,
> d) det er frivillig å gi fra seg opplysningene, og
> e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28."

Informasjonskravet er også formulert i cookiedirektivet. Det følger av artikkel 5 (3) at brukeren skal ha "been provided with clear and comprehensive information". For øvrig henvises det til samtykkereglene i personverndirektivet. I personverndirektivet artikkel 10

er det gitt regler om hvilken informasjon som skal gis brukeren der behandlingsansvarlige henter opplysninger direkte fra ham eller henne. Denne bestemmelsen svarer i all hovedsak til bestemmelsen i personopplysningsloven § 19.

Personvernnemnda har i en sak fra 2009 om drosjeløyver uttalt at den som avgir samtykket "må informeres konkret om hvilke opplysninger som skal innhentes for å kunne sies å være tilstrekkelig informert."[133] Det later til at nemnda i vedtakets begrunnelse stiller krav om et høyt presisjonsnivå på informasjonen som gis av den behandlingsansvarlige. Et informert samtykke innebærer at brukeren "må forstå hva erklæringen gjelder, og hvilke konsekvenser denne får eller kan få".[134] Når det gjelder lagring av cookies, kan det være vanskelig å informere brukeren tilstrekkelig om dette, ettersom de fleste har forholdsvis liten forståelse for de tekniske prosessene som ligger bak grensesnittet. Utfordringen ligger i å informere brukeren om de faktiske prosessene og hvordan de henger sammen, uten å bli så detaljert at man mister brukeren underveis. Dersom brukeren mister oversikten vil han eller hun lettere gi opp, noe som kan resultere i resignasjon og et i realiteten uinformert samtykke. I cookiedirektivets fortale nummer 66 er det formulert et formål om at informasjonen skal være så brukervennlig som mulig. Dette er et svært viktig poeng, ettersom dagens situasjon ikke helt samsvarer med dette brukervennlighetskravet. Særlig er dette tilfelle for personvernpolicyer. Mange hevder at disse er utformet på en måte som gjør dem unødig kompliserte eller uforståelige for brukerne.[135] Dette kan tenkes å stride mot kravet om at informasjonen skal være presentert på en klar og forståelig måte. For det første er det ofte vanskelig å finne frem til dokumentene eller nettsidene hvor avtalene presenteres. Google presenterer for eksempel sin personvernpolicy på en svært komplisert måte. Deres policy har en generell del som gjelder for alle tjenestene, mens hver tjenestetype i tillegg har en egen policy som presenteres i et separat dokument.[136] De spesielle reglene er altså ikke presentert etter tjenestens navn, men etter tjenestenes

---

[133] PVN-2009-16 Drosjeløyve.
[134] NOU 1997-19 Et bedre personvern, merknad til § 2.
[135] Jensen (2004) s. 471.
[136] Link til Googles personvernpolicy: http://www.google.com/intl/en/privacy/.

egenskaper. Dette gjør det vanskelig å navigere mellom de forskjellige policyene som gjelder for den enkelte tjenesten. Det kan argumenteres for at Googles samlede personvernpolicy er så vanskelig å navigere i at den ikke oppfyller kravet til en klar og forståelig presentasjon.

Mange typer personvernpolicy er videre ofte komplisert utformet. De bruker ofte et språk fylt med juridiske eller tekniske begrep som ikke defineres og sammenhengene er ofte vanskelig å forstå. Som et resultat er det en stor andel av brukerne som ikke med rimelighet kan forventes å forstå disse tekstene.[137]

Presisjonsnivået i personvernpolicyer kan også ofte være dårlig. Svært mange slike avtaler nevner kun at enkelte typer informasjon deles med tredjeparter, uten å presisere hvilke tredjeparter det dreier seg om, hvilken informasjon som deles eller hva som er formålet med dette. Ofte henvises brukeren for eksempel til å lese gjennom en personvernpolicy hos tredjeparten for å finne ut mer om deres bruk av opplysningene, uten at brukeren har fått fullstendig informasjon om hvem denne tredjeparten er. I undersøkelsen av brukerprofilering på levis.com fant Dwyer for eksempel at nesten ingen av tredjepartene som Levi's delte brukeropplysninger med var navngitte i deres personvernpolicy.[138]

Det bør presiseres at informasjonskravet innebærer at brukeren skal ha hatt tilgang til informasjon om og rundt lagringen av cookies *før* han eller hun samtykker. Det stilles altså krav om at både informasjonen og samtykket gis forut for lagring av cookies.

4.4 Tilbakekall av samtykke

Det følger av personopplysningslovens forarbeider at samtykke til behandling av personopplysninger når som helst kan kalles tilbake.[139] I så fall kan den behandlingen som

---

[137] Jensen (2004) s. 475.
[138] Dwyer (2009) s. 7.
[139] Ot.prp. nr. 92 (1998-1999) s. 104.

samtykket retter seg mot, ikke fortsette. Dette er en følge av at samtykket skal være frivillig avgitt. Det må være rom for å feile og å forandre mening uten at dette skal gå ut over den enkelte.[140] Dette kan imidlertid ikke få konsekvenser for allerede behandlet materiale. Behandling som har skjedd mellom avgivelsen og tilbaketrekningen av samtykket, vil fremdeles være lovlig.[141] Forbudet mot å fortsette behandling av personopplysninger må videre modereres i tilfeller hvor samtykke ikke lenger kreves for behandlingen. Dersom det foreligger lovgrunnlag eller en nødvendighetsgrunn som presisert i personopplysningsloven § 8, er det ikke lenger nødvendig for behandling at den registrerte har samtykket.[142] Det stilles ikke noe krav i personopplysningsloven om at behandlingsgrunnlaget må være det samme gjennom hele behandlingsperioden. Det er videre anbefalt i forarbeidene at man i størst mulig grad skal søke å innhente samtykke til behandling.[143] Dette kan føre til at mange behandlingsansvarlige innhenter samtykke fra den registrerte selv om det foreligger andre behandlingsgrunnlag. I slike tilfeller kan man ikke stille krav om at behandlingen skal opphøre selv om det på forhånd var innhentet et samtykke fra den registrerte.

Det oppstår imidlertid noen problemer når regelen om tilbakekall av samtykke anvendes for lagring og behandling av cookies. Det kan det for eksempel svært vanskelig å trekke tilbake et samtykke når behandlingen gjøres av en tredjepart som brukeren ikke kjenner. Dette kan være tilfelle hvor behandlingsansvarlige ikke har gitt tilstrekkelig informasjon i sin personvernpolicy om hvem de deler opplysningene med. Enkelte nettsteder setter mange cookies som de deler med flere forskjellige tredjeparter, og det er ofte vanskelig å få oversikt over den totale mengden opplysninger som lagres. Dette kan føre til at brukere som gir uttrykk for at de trekker tilbake sitt samtykke, ikke gjør dette på en tilstrekkelig spesifisert måte, og dermed at enkelte cookies fortsatt blir lagret og behandlet.

---

[140] Johansen (2001) s. 78.
[141] Ot.prp. nr. 92 (1998-1999) s. 108.
[142] Coll (2000) s. 44.
[143] Ot.prp. nr. 92 (1998-1999) s. 108.

4.5 Særlig om innstillinger i brukerens nettleser

Et tema som særlig har vært diskutert i den offentlige debatten om cookiedirektivet, er hvordan direktivet skal gjøres gjeldende for samtykke gjennom nettleserinnstillinger. Kravet om samtykke til lagring og behandling av cookies anses i praksis oppfylt gjennom brukerens nettleserinnstillinger.[144] Spørsmålet er om denne praksisen må endres etter de nye reglene i cookiedirektivet, og i tilfelle hvordan.

Kravet til samtykke i norsk rett er, som presisert og utdypet i de foregående kapitlene, at det skal foreligge "en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv".[145] Oppfylles dette kravet i praktiseringen av forhåndsdefinerte nettleserinnstillinger som godtar lagring og behandling av cookies i brukerens utstyr?

Frivillighetskravet innebærer at samtykket ikke skal gis under noen form for tvang eller tvangslignende situasjoner, jamfør kapittel 4.3.2.1. Det kan argumenteres for at selve nedlastingen eller kjøpet av et nettleserprogram innebærer samtykke til lagring, ved at man samtykker til de innstillinger som på forhånd er definert. Dette ville imidlertid neppe være tilfelle der nettleseren følger med i pakken når brukeren kjøper utstyret, uten at dette spesifikt er opplyst. Videre er kravet om at det skal foreligge en uttrykkelig erklæring, problematisk. Når en bruker samtykker til å laste ned eller kjøpe en nettleser, er det ikke de foranderlige innstillingene han eller hun samtykker til, men de faste innstillingene og applikasjonene som nettleseren tilbyr. Brukeren har ikke anledning til å gi et samtykke som spesifikt retter seg mot at de forhåndsdefinerte innstillingene godtar lagring og behandling av cookies. Dette gjør at samtykket ikke kan anses som uttrykkelig. Det kan stilles spørsmål om brukeren ved bruk av nettleseren uten å endre på innstillingene kan sies å ha samtykket til disse. Dette dreier seg eventuelt om samtykke ved konkludent atferd. Etter pasientrettighetsloven kreves det at det tydelig fremgår om pasienten mente å samtykke

---

[144] Dette praktiseres av de fem største nettleserne: Internet Explorer, Safari, Firefox, Google Chrome og Opera.
[145] Personopplysningsloven § 2 nr. 7.

med sin atferd for at samtykke ved konkludent atferd skal godtas.[146] Slik atferd på nett er det imidlertid vanskelig å vurdere. Det kan være mange grunner til at brukeren tar nettleseren i bruk før han eller hun eventuelt endrer på innstillingene, og man kan ikke anta at brukeratferden innebærer et samtykke til lagring av cookies. Mangelen på informasjon rundt lagring og behandling av cookies vil også gjøre det vanskelig å anta at brukeren har gitt et informert samtykke. Kravet til informasjon er strengt. Brukeren skal som nevnt i kapittel 4.3.2.3. ha hatt tilgang til informasjon om lagring av cookies før han eller hun samtykker til lagring. Denne informasjonen er vanskelig å tilegne seg før man faktisk begynner å bruke en nettleser. Det er etter dette tvilsomt om de tre hovedvilkårene for samtykke (frivillighet, uttrykkelighet og informasjon) er oppfylt ved et samtykke gjennom nedlasting, kjøp eller bruk av en nettleser.

I sin uttalelse om samtykkedefinisjonen hevder Artikkel 29-arbeidsgruppen at samtykke basert på brukerens manglende handling ikke imøtekommer kravet om et utvetydig samtykke.[147] Dette gjelder for eksempel ved bruk av forhåndsdefinerte nettleserinnstillinger som godtar profilering og reklameretting mot brukeren gjennom lagring av cookies.[148] Dette standpunktet har også vært uttrykt i en tidligere uttalelse fra arbeidsgruppen om internettbasert atferdsrettet reklame, hvor de hevder at det må være særlig viktig for nettlesere å tilby forhåndsdefinerte innstillinger som ikke godtar lagring av cookies eller sender tredjepartscookies.[149]

Når det gjelder lagring av cookies på brukernes datautstyr, er det vanligste i dag likevel å anse samtykke for å være oppnådd gjennom innstillinger i brukerens nettleser. Også i cookiedirektivet kommer dette frem. I direktivets fortale nummer 66 er det blant annet gitt uttrykk for at innstillinger i brukerens nettleser kan godtas som et samtykke der dette er

---

[146] NOU 2005:1 s. 71.
[147] Article 29 Data Protection Working Party: WP 187 (2011) s. 12.
[148] Id.
[149] Article 29 Data Protection Working Party: WP 171 (2010) s. 15.

teknisk mulig og effektivt, og i overensstemmelse med personverndirektivets regler.[150] Spørsmålet om hvilke krav som eventuelt skal stilles til innstillinger i nettlesere for at de skal skal oppfylle direktivets samtykkekrav er enda ikke drøftet utførlig av Kommisjonen. Artikkel 29-arbeidsgruppen har imidlertid i sin uttalelse om atferdsrettet reklame uttrykt sine meninger rundt spørsmålet, og er kommet til at det må stilles forholdsvis strenge krav til en nettleser for at innstillingene til lagring av cookies skal anses å uttrykke brukerens samtykke.[151] Det kan hevdes at den "opt ut"-løsningen som i dag velges av de fleste nettleserne og nettsidene innebærer passivt samtykke som etter personopplysningsloven ikke skal godtas. En "opt inn"-løsning vil derimot trolig kunne anses som et aktivt samtykke etter personopplysningsloven.

5 Norsk implementering av cookiedirektivet

5.1 Gjeldende relevant lovgivning

I kapittel 3 er innholdet i cookiedirektivet presentert, med særlig fokus på kravet som stilles til samtykke til lagring av cookies. Videre er samtykkekravet i norsk rett drøftet i kapittel 4. For å kunne vurdere hvordan implementeringen av de nye cookiereglene bør og kan gjøres i Norge, er det nødvendig å ha kjennskap til de regler som allerede gjelder.

Bestemmelsene som er relevante for samtykke til lagring og behandling av cookies, er nedfelt i ekomloven og ekomforskriften. Ekomloven gir regler for "virksomhet knyttet til overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner", jamfør § 1-2. Loven har et teknologinøytralt utgangspunkt og omfatter "alle typer elektronisk kommunikasjonsteknikk, virksomhet og myndighetsutøvelse i forbindelse med bruk og utvikling av slik kommunikasjon".[152] Begrepet "elektronisk kommunikasjon"

---

[150] Direktiv 2009/136/EF, fortale nummer 66.
[151] Article 29 Data protection Working Party:WP 171 (2010) s. 13 flg.
[152] Ot.prp. nr. 58 (2002-2003) s. 84.

er definert i § 1-5 som "overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel i et system for signaltransport". Det har ingen betydning for definisjonen hvilken type informasjon som overføres, og definisjonen innebærer dermed både personopplysninger og andre opplysninger.[153] Formålet med ekomloven er etter § 1-1 å "sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, gjennom effektiv bruk av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse, samt stimulere til næringsutvikling og innovasjon".

Det er klart at ekomloven gjelder for alle typer internettvirksomhet, ettersom denne typen virksomhet alltid innebærer en form for overføring av elektronisk kommunikasjon. Ettersom lagring av cookies er avhengig av internettvirksomhet, gjør bestemmelsene i ekomloven seg gjeldende for denne drøftelsen. Forskriften som er knyttet til ekomloven, ekomforskriften, gjelder etter § 1-1 "rettigheter og plikter for tilgang for tilbydere og andre brukere til elektronisk kommunikasjonsnett og tilbud av elektronisk kommunikasjonstjeneste". Forskriften gjelder altså konkrete rettigheter og plikter i forbindelse med bruken av elektronisk kommunikasjon, mens ekomloven gir regler for denne typen virksomhet i videre forstand. Forskriften gjelder for både fysiske og juridiske personer, jamfør "tilbydere og andre brukere".

I dag reguleres spørsmålet om cookies gjennom ekomforskriftens kapittel 7 om kommunikasjonsvern mv. Av § 7-3 følger en bestemmelse om behandling av informasjonskapsler mv.:

> "Elektronisk kommunikasjonsnett kan ikke benyttes til lagring av opplysninger i brukers kommunikasjonsutstyr eller for å skaffe seg adgang til slike, uten at bruker er gitt informasjon av den behandlingsansvarlige i henhold til personopplysningsloven , herunder om behandlingsformålet og er gitt anledning til

[153] Ot.prp. nr. 58 (2002-2003) s. 86.

å motsette seg behandlingen. Dette er likevel ikke til hinder for teknisk lagring eller adgang til opplysninger:

1. utelukkende for det formål å overføre eller lette overføringen av kommunikasjon i et elektronisk kommunikasjonsnett
2. som er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel."

Bruk av cookies er en måte å lagre opplysninger i en brukers kommunikasjonsutstyr, og er dermed omfattet av regelen. Det følger også av bestemmelsens overskrift, "Informasjonskapsler mv.", at cookies er omfattet. Bestemmelsen sier at lagring av (eller det å skaffe seg adgang til) opplysninger kun er tillatt dersom det er gitt informasjon om lagringen, herunder behandlingsformålet, og brukeren er gitt anledning til å motsette seg lagring. Hovedregelen etter nåværende bestemmelse er altså at lagring av cookies er tillatt så lenge man informerer om, og gir mulighet til å nekte lagringen. Det sies ingenting om kravene til informasjon eller om hvordan nekting av lagring skal foregå. I praksis medfører dette at de fleste nettsider som setter cookies kan velge å bruke informasjonsmetoder som i størst mulig grad fører til at brukerne unngår å slette cookies.

Det gjøres i forskriftens § 7-3 enkelte unntak for kravet om samtykke. For det første er teknisk lagring unntatt samtykkekravet. Dette innebærer at lagring av cookies som er nødvendig for den tekniske funksjonaliteten til en nettside eller tjenester som tilbys ikke krever brukerens samtykke. Lagring i forbindelse med overføring av kommunikasjon eller leveringen av uttrykkelig forespurte informasjonstjenester, er også unntatt samtykkekravet. Ettersom disse unntakene fra samtykkekravet som følger av ekomforskriften § 7-3 sjelden vil gjøre seg gjeldende for behandlingen av cookies til kommersielle formål. Derfor vil jeg ikke drøfte unntaksbestemmelsene nærmere.

5.2 Forslag til endringer i ekomloven og ekomforskriften

Den 25. juni 2010 ble det foreslått endringer i ekomloven og ekomforskriften. Forslaget er i november 2011 fortsatt under behandling.[154] Det er for det første foreslått en endring i ekomlovens saklige virkeområde. Loven skal etter forslaget gjelde for "virksomhet knyttet til elektronisk kommunikasjon, herunder bruk av elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste med tilhørende fasiliteter, tilhørende tjenester og utstyr."[155] Dette er en mye videre definisjon av lovens virkeområde enn den som er inntatt i den nåværende bestemmelsen, og dette er gjort bevisst for å ta høyde for den fremtidige tekniske utviklingen på dette området.[156]

Det er videre utarbeidet et forslag til endring i ekomforskriften § 7-3. Forslaget tar sikte på å gjennomføre endringene i EUs "telekompakke", deriblant cookiedirektivet. Det er blant annet foreslått endringer i ekomforskriften § 7-3, som i forslaget er endret til følgende tekst:

> "§ 7-3 Opplysninger i brukers kommunikasjonsutstyr
>
> Lagring av opplysninger i brukers kommunikasjonsutstyr eller å skaffe seg adgang til slike opplysninger er ikke tillatt. Slik lagring eller adgang kan likevel skje dersom bruker har blitt informert av den behandlingsansvarlige i henhold til personopplysningsloven og har gitt sitt samtykke. Første punktum er likevel ikke til hinder for teknisk lagring eller adgang til opplysninger:
>
> 1. utelukkende for det formål å overføre eller lette overføringen av kommunikasjon i et elektronisk kommunikasjonsnett
> 2. som er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel"

---

154 Samferdselsdepartementet (2010), høringsnotat s. 15.
155 Id.
156 Id.

Etter den foreslåtte bestemmelsen er hovedregelen ikke lenger at lagring av cookies kan skje, men derimot at slik behandling ikke er tillatt. Videre gjøres en eventuell lagring avhengig av brukerens informerte samtykke, noe som ikke er nødvendig etter dagens ordlyd. For definisjonen av det informerte samtykket er det henvist til bestemmelsene i personopplysningsloven, som skal gjelde også her. Dette betyr at drøftelsen om det informerte samtykket fra kapittel 5 vil være aktuell for tolkningen av den foreslåtte § 7-3 i ekomforskriften.

Dersom de foreslåtte cookiereglene vedtas, vil dagens praktisering av behandling og kravet til innholdet i en personvernpolicy måtte endres vesentlig. Man må finne løsninger for lagring og behandling som innebærer at brukeren aktivt må godta cookies som krever brukerens samtykke. Dette betyr at forhåndsdefinerte innstillinger i nettlesere ikke lenger kan godta lagring og behandling av cookies som etter loven krever brukerens samtykke. Jeg vil i kapittel 5.5.2. presentere noen av løsningene som hittil er foreslått.

5.3 Tilsyn og håndheving

Et viktig spørsmål for implementeringen av cookiedirektivet er hvordan reglene skal håndheves. Som nevnt i kapittel 3.4.1. er det anbefalt at medlemslandene oppretter egne tilsynsmyndigheter for kontroll og håndheving av de nye reglene. Hvordan man i Norge skal organisere opprettelsen av en egen myndighet som foreslått i cookiedirektivet, artikkel 15 (a) er det enda ikke tatt stilling til.

I Norge har blant annet *Datatilsynet* denne typen funksjon i dag. Etter personopplysningsloven § 42 har de blant annet som oppgave å kontrollere og sørge for at regelverket for behandling av personopplysninger blir fulgt. Tilsynet er også høringsinstans i personvernsaker og kan treffe vedtak. Videre fungerer Datatilsynet som ombudsmann for personvernspørsmål,[157] og det er de som mottar og behandler meldeskjema og konsesjonssøknader for behandling av personopplysninger. En annen aktør som kan

[157] Direktoratet for forvaltning og IKT (2011) s. 19 flg.

fungere som tilsynsmyndighet, er *Post- og Teletilsynet*. Tilsynet er et frittstående forvaltningsorgan underlagt Samferdselsdepartementet.[158] Arbeidsområdene deres er å regulere og overvåke den norske sektoren for post og elektronisk kommunikasjon. De vil dermed kunne spille en viktig rolle for reguleringen av de nye ekom-reglene. Videre vil også *Forbrukerombudet* kunne være sentrale i arbeidet med å føre tilsyn med cookiereglene. Forbrukerombudets oppgaver er å sikre forbrukernes interesser ved å føre tilsyn med at markedsføring og standard kontraktsvilkår er i samsvar med markedsføringsloven.[159] Bruken av cookies er særlig problematisk i forbindelse med brukerprofilering og markedsføring. Forbrukerombudet har særlig kompetanse på disse områdene, og vil være en naturlig aktør i arbeidet med å sikre at reklamebransjen oppfyller de nye kravene til innhenting av brukersamtykke.

En mulig løsning for den norske implementeringen av cookiedirektivet kan være å gi de tre nevnte organene separate tilsynsoppgaver etter virksomhetsområde. Dermed vil man få tre separate tilsynsmyndigheter som har ansvar for tilsyn og kontroll av direktivet. En annen løsning vil være å opprette et nytt tilsyn for kommunikasjonsvern, noe som ikke synes særlig aktuelt.

En organisasjon som er opprettet på EU-nivå for kontroll- og tilsynsformål, er The European Regulators Group for electronic communications networks and services (BEREC).[160] Denne gruppen ble opprettet av Kommisjonen i forordning 1211/2009.[161] Etter reguleringen skal BEREC fungere som et uavhengig rådgivende organ og også et forum for samarbeid mellom de nasjonale tilsynsmyndighetene og Kommisjonen. Det kan tenkes at organisasjonens råd og innspill vil være viktig for de norske prosedyrene for kontroll og håndheving av cookiedirektivet.

---

158 http://www.npt.no/.
159 http://www.forbrukerombudet.no/om-forbrukerombudet.
160 Samferdselsdepartementet (2010), høringsnotat s. 2.
161 Id.

Man kan også stille spørsmål ved om det burde opprettes et eget organ for selvregulering i reklamebransjen, som kunne fungere som en bransjeorganisasjon, normsetter og mellomledd mellom tilsynsmyndighetene og reklamebransjen. Dette er en løsning som er valgt i mange europeiske land, ved at man har opprettet nasjonale selvreguleringsorganisasjoner med medlemskap i EASA.[162] Også EU-kommisjonen ved kommissær Neelie Kroes stiller seg positiv til slike ordninger.[163] Nesten alle landene i Europa har egne selvreguleringsorganisasjoner, med unntak av Danmark, Latvia og de fleste landene på Balkan.[164] Norge har ikke selvregulerende medlemsorganisasjoner i EASA, men *Interesseorganisasjonen for interaktiv markedsføring* (INMA) kan indirekte sies å være medlem gjennom IAB Europe.[165] INMA hevder at de vil komme til å følge retningslinjene for selvregulering av atferdsrettet reklame som er publisert av EASA, men at de ikke vil komme til å fungere som en selvreguleringsorganisasjon.[166] Dette forklarer daglig leder i INMA, Anders Willstedt, med at Norge er et svært lite indre reklamemarked, og de fleste aktørene som driver med atferdsrettet reklame er internasjonale bedrifter som følger retningslinjene for sine respektive land.[167] Han mener altså at det ikke er behov for en selvreguleringsorganisasjon for (atferdsrettet) reklame i Norge. INMA fører likevel tett dialog med de europeiske selvreguleringsorganisasjonene om etterfølging av bransjens retningslinjer.

5.4 Reaksjoner på de nye cookiereglene

De nye cookiereglene har fått en del oppmerksomhet fra media og IT-bransjen i Norge. Dette har sammenheng med at lagring av cookies er en svært utbredt og vanlig aktivitet for internettaktørene, og at endringen i reglene rundt denne lagringen potensielt vil få store konsekvenser for mange av dem, både juridisk og økonomisk.

---

[162] European Advertising Standards Alliance.
[163] Kroes (2011).
[164] EASA [2](2011).
[165] http://www.inma.no/.
[166] Willstedt (2011).
[167] Id.

Diskusjonen dreier seg, også i media, om hvilke krav som skal/kan stilles til brukernes samtykke til behandling av personopplysninger. IT- og reklamebransjene mener at et strengt praktisert samtykkekrav svært vanskelig vil la seg gjøre ettersom det i praksis lagres flere titall forskjellige typer cookies for hver nettside en bruker klikker seg inn på. Dersom samtykke skal innhentes for hver cookie, er argumentet at brukeren vil bruke mer tid på å gi sitt samtykke til disse enn han eller hun faktisk bruker på siden. Dette kan føre til motvilje fra brukerne, som med dette får en langt dårligere brukeropplevelse.

INMA og *Mediebedriftenes Landsforening (MBL)* stiller seg svært negative til endringen i ekomforskriften. De hevder i sin høringsuttalelse til Samferdselsdepartementet at en så streng regulering av lagring av cookies som den foreslåtte forskriften innebærer vil medføre økonomiske konsekvenser for norsk næringsliv som følge av en økt konkurranse med de landene som ikke innfører så strenge regler som Norge.[168] Organisasjonene mener videre at det etter § 7-4 burde være en mulighet til å samtykke via innstillinger i nettleser. De ber departementet om å innta en presisering i implementeringen om at lov- og forskriftsendringene ikke medfører noen endring i gjeldende rett med hensyn til blant annet bruk av cookies, samt en presisering av at dagens forhåndsdefinerte nettleserinnstillinger er å anse som tilstrekkelige til å oppfylle samtykkekravet.

De aller fleste cookies som settes på nettsider har imidlertid nødvendige tekniske formål og vil dermed ikke vil behøve samtykke for lagring etter den foreslåtte forskriften. Det er i praksis kun de cookiene som settes med reklameformål eller andre kommersielle formål for øyet, som vil berøres av kravet om samtykke. Dette følger av § 7-3, 1.ledd 3.pkt nr. 1 og 2. De fleste teknisk motiverte cookies, slik som autentiseringscookies og cookies som muliggjør elektroniske handlekurver, vil kunne unntas samtykkekravet etter det første alternativet. Informasjonssamfunnstjenester[169] omfatter blant annet e-post, søkemotorer,

---

[168] INMA/Mediebedriftenes landsforening (2011) s. 1.
[169] Definert i ehandelsloven § 1.

gratis musikk-, video- eller spilltjenester, og næringsdrivendes nettsteder.[170] Forslaget innebærer at også disse aktørene er unntatt kravet om å innhente samtykke så lenge behandlingen er nødvendig for å levere tjenester som brukerne deres uttrykkelig har forespurt.

Daglig leder i INMA, Anders Willstedt, har likevel i et intervju med E24 uttalt at de nye reglene vil "slå bena under inntjeningen til norske nettmedier".[171] For å illustrere de negative konsekvensene cookiereglene kan få for brukerne, har organisasjonen laget en demonstrasjon som viser hvordan de mener en vanlig nettside vil fungere dersom cookiereglene blir implementert slik de er foreslått i ekomforskriften § 7-3.[172] I demonstrasjonen er det lagt inn "popup"-vinduer for hver cookie som lagres på nettsiden, og man må for hvert vindu velge om man vil akseptere cookien for å komme til nettsiden. Dersom man ikke godtar cookiene, vil nettsiden ikke fungere, og brukeren får opp en feilmelding som sier at siden ikke kan åpnes. Dette er etter min mening en ekstremversjon av hva cookiedirektivet innebærer, og jeg er usikker på om denne demonstrasjonen er særlig betegnende for hvordan internettopplevelsen vil bli med de nye reglene. Cookies som kun er relatert til teknisk lagring faller som nevnt utenfor kravet om samtykke fra brukeren. Videre brukes det i demoen cookies som er relatert til markedsføring, og nekting av disse cookiene bør ikke, teknisk sett, kunne føre til at nettsiden ikke fungerer optimalt. Det er heller ikke gitt at løsningen med "popup"-vinduer vil være den eneste som tilfredsstiller direktivkravene.

Demonstrasjonen er likevel et godt eksempel på holdningen reklamebransjen har til cookiedirektivet, og argumentet om brukervennlighet er et argument man finner i mange kommentarer fra reklamebransjens støttespillere i forskjellige intervjuer og artikler på nett. I en artikkel fra E24 er flere aktører fra medie- og reklamebransjen intervjuet om de nye

---

[170] Ot.prp.nr.31 (2002-2003) s. 55.
[171] Henriksen [1](2011).
[172] INMA (2011).

cookiereglene og den norske implementeringen av disse.[173] Kommunikasjonsrådgiver Øyvind Solstad fra mediebyrået Carat mener de nye cookiereglene er "gammeldags, inkompetent og næringsfiendtlig", og mener at et krav om samtykke til enhver type cookie vil føre til kaos for nettsider og deres brukere.[174] Åsta Bråthen, som er daglig leder i mediebyrået IUM, mener de nye reglene kan "føre til at brukeropplevelsen vil kunne bli dårligere".[175] Torstein Rafgård, byråsjef i mediebyrået OMD, hevdet i samme artikkel at "Endringen vil eventuelt medføre at annonsørene mister muligheten til å måle medieinvesteringene direkte. (…) For konsumentene vil dette medføre mindre relevante annonser og dermed en redusert brukeropplevelse av nettsidene."[176] Medie- og reklamebransjens innvendinger dreier seg stort sett om den negative økonomiske effekten de nye reglene vil ha på markedsføringsnæringen, og i tillegg den negative effekten de vil få på brukeropplevelsen på nett. Det synes ikke å være særlig mye fokus på beskyttelse av personvernet fra disse aktørene.

Forbrukerombudet stiller seg på den annen side svært positive til endringsforslaget til ny § 7-3 i ekomforskriften. De mener at et eksplisitt samtykke fra brukeren vil kunne bidra til å minske faren for lagring av skadelig programvare i brukernes kommunikasjonsutstyr. Ombudet foreslår imidlertid en klargjøring av hvordan bestemmelsen skal håndheves, og at det bestemmes hvilket organ som skal føre tilsyn med bestemmelsen.[177]

Post- og Teletilsynet ser ut til å godta hoveddelen av innholdet i forskriftens foreslåtte § 7-3. De presiserer imidlertid at det ikke følger av direktivet at man kan gjøre unntak fra hovedregelen om samtykke for å "lette overføringen" av kommunikasjon – og ber derfor om at dette alternativet tas ut av bestemmelsens nr. 1.[178] Post- og Teletilsynet går altså inn

---

[173] Henriksen [2](2011).
[174] Id.
[175] Id.
[176] Id.
[177] Forbrukerombudet (2010) s. 26.
[178] Post- og Teletilsynet (2010) s. 23.

for en noe strengere regel enn den foreslåtte bestemmelsen innebærer, ettersom de foreslår en innskrenking i unntakene fra hovedregelen om samtykke.

Etter reaksjonene fra næringslivet og sivilsamfunnet å dømme, er det kravet til samtykke som er det største stridsspørsmålet rundt de nye reglene som følger av cookiedirektivet. Det er vanskelig, men også avgjørende, for en vellykket implementering av direktivet å komme frem til en klar og entydig forståelse av hva som ligger i samtykkekravet. Det er imidlertid svært få av høringsinstansene som har hatt innsigelser til den foreslåtte § 7-3 i ekomforskriften. Dette må man kunne tolke dithen at de støtter forslaget og de implikasjonene det vil ha. Det har ikke skjedd noe i implementeringsprosessen siden høringsuttalelsene ble fremlagt i september 2010. Det arbeides fortsatt med utkastet til lovproposisjonen i Samferdselsdepartementet. Det er derfor ikke tatt endelig stilling til hvordan bestemmelsene om cookies skal utformes. Det er ventet at et endelig lovforslag skal legges frem for Stortinget vårsesjonen 2012.[179]

5.5 Tekniske løsninger – personvern gjennom arkitektur?

Teknologisk arkitektur har i praksis stor betydning for praktiseringen av rettsregler på IT-rettens område. Jacobs har uttrykt viktigheten av teknologisk arkitektur slik:

> "The (information) architecture determines how information flows within a particular IT-system: who can see what about whom. Since knowledge about others gives a stronger position and thus more power, IT-architecture is a highly political matter. After all, centralised informational control supports centralised societal control"[180]

I cookiedirektivets fortale nummer 9 ligger et mål om at medlemslandene skal samarbeide for å introdusere og utvikle relevant teknologi hvor dette er nødvendig for å oppfylle

---

[179] Wongraven (2011).
[180] *Data Protection in a Profiled World* (2010) s. 291.

målsettingen med å minimere behandlingen av personopplysninger og i størst mulig grad anonymisere behandlingsprosesser. Dette kan tolkes som et ønske om å oppnå den harmonien mellom lovregler og teknologisk arkitektur som blant annet er nevnt i kapittel 1.1.

Det er foreslått flere løsninger til samtykkeproblematikken som alle innebærer en harmonisering mellom arkitektur og lovgivning. En løsning som særlig er lovpriset av jurister, har fått tilnavnet *"privacy by design"* (personvernvennlig design). Etter denne løsningen bygges personvern inn i teknologien fra starten av, altså ved utformingen av teknologien som tillater lagring av personopplysninger. [181] Det er blant annet foreslått at man innfører systemer hvor uavhengige mellomaktører lagrer opplysningene som samles fra brukerne og videre formidler disse til aktører som behandler opplysningene. Slik vil ikke de behandlingsansvarlige samtidig være lagringsansvarlige, noe som vil kunne vanskeliggjøre at opplysninger blir misbrukt eller kommer på avveie.[182] Det finnes imidlertid mange måter å implementere "privacy by design". Poenget er at vernet om personopplysninger må ligge innebygd i teknologien, og utviklere og teknologer må være bevisste på å la spørsmålet om vern av personopplysninger være en integrert del av utforming og utvikling av produktene sine. Mange av de europeiske datatilsynsmyndighetene, deriblant Datatilsynet og The European Data Protection Supervisor (EDPS – den europeiske dataombudsmannen), stiller seg positive til "privacy by design"-løsningen.[183]

En annen løsning kan være å utvikle personvernfremmende teknologi (Privacy Enhancing Technologies, eller PET). Personvernfremmende teknologier er tekniske løsninger og teknologier som er utviklet med det spesifikke formål å beskytte personvernet til brukere og andre internettaktører.[184] Et eksempel på personvernsfremmende teknologier er

---

[181] *Data Protection in a Profiled World* (2010) s. 323 flg.
[182] *Data Protection in a Profiled World* (2010) s. 324.
[183] Talberg-Furulund (2010).
[184] Cannon (2005) s. 17.

anonymiseringsverktøyene, som blant annet kan brukes til å sette opp anonym nettsurfing eller anonyme e-postkonti. Et annet, og kanskje mer velkjent eksempel, er verktøyene man kan bruke for å slette historie i nettlesere.[185] Forskjellen mellom personvernfremmende teknologier og "privacy by design"-løsninger er at de personvernfremmende teknologiene tar utgangspunkt i personvernsproblemer som allerede ligger i eksisterende teknologi, og søker å bøte på problemene gjennom ny teknologi. Etter "privacy by design"-løsningen må man ikke lage programmer for å sikre personvernet i andre programmer. Her bygger utviklerne personvernet inn i teknologien fra starten av og i vedlikeholdet av teknologien.

Et mer konkret og samtidig mer vidtomfavnende løsningsforslag er den såkalte "*Do Not Track"*-tilnærmingen. Denne løsningen har fått større tilslutning fra de store internettaktørene, som Google, Microsoft, Adobe og Facebook. "Do Not Track" er en webstandard som gir brukeren muligheten til å gi uttrykk for at han eller hun ikke ønsker sine bevegelser på nett sporet på tvers av nettsteder. Dette gjøres gjennom nettleseren, ved at det legges til en "Do Not Track"-spesifikasjon i "headeren" til nettleserens adressefelt. Denne "headeren" gir blant annet annonse- og innholdsleverandører signal om at brukeren ikke ønsker å bli sporet på tvers av nettsteder.[186] Firefox, Safari og Internet Explorer har allerede begynt å tilby brukerne sine valget om å bruke slike spesifikasjoner.[187]

I samarbeid med forskjellige store internettaktører og interessegrupper har *World Wide Web Consortium (W3C)* opprettet en arbeidsgruppe for beskyttelse mot brukersporing (Tracking Protection Working Group).[188] Gruppen har medlemmer fra noen av de største internasjonale internettaktørene i tillegg til eksperter på området, og den er opprettet for å arbeide for standardisering av "Do Not Track"-teknologi. Arbeidsgruppen publiserte i november 2011 et arbeidsdokument om "Do Not Track",[189] som inneholdt forslag til to standarder som etter hvert skal implementeres av alle medlemmene i arbeidsgruppen. Også

---

[185] Cannon (2005) s. 19 flg.
[186] W3C (2011).
[187] http://donottrack.us/.
[188] W3C (2011).
[189] W3C (2011).

EU-kommisjonen stiller seg positiv til arbeidet med "Do Not Track", og kommisjonær Neelie Kroes uttrykte i en tale fra 22. juni 2011 sine høye forhåpninger til "Do Not Track"-teknologien.[190] I samme tale etterlyste hun en standardisering av disse teknologiene, et arbeid som nå altså er igangsatt.

Det finnes selvfølgelig mange flere forslag til tekniske løsninger for å bevare personvernet gjennom arkitektur. De løsningene som er presentert her, er de som hittil synes å ha fått størst oppslutning. Dette kan ha sammenheng med at de er systemorienterte løsningsforslag som vil kunne brukes i mange forskjellige situasjoner.

[190] Kroes (2011).

6 Avslutning og konklusjon

IT-bransjen, reklamebransjen og massemedia har de siste årene tjent godt på informasjonshandelen, noe blant annet en manglende regulering av handel med informasjon på internett har tillatt. Næringslivet har hittil (i stor grad) kunnet bruke cookies til å skaffe seg personopplysninger som de bruker til kommersielle formål. En innarbeidet praksis hvor dette er tillatt bør imidlertid ikke tilsi at lovgiverne unnlater å gjøre endringer som vil påvirke denne praksisen. I boka *Til forsvar for personvernet* beskriver Georg Apenes dagens praktisering av informasjonshandel på nett slik:

> "Det er en moderne variant av det gamle norske hovedprinsippet, som lærer oss at gammel urett kan bli rett når den (uretten) sørger for å alliere seg med passivitet. Og både i krig og politikk finnes gode eksempler på at utmattelse vil føre frem dersom det ikke haster."[191]

Apenes har et viktig poeng. Man ikke kan tillate at kompleksiteten som ligger i regulering av "lovløs" teknologi fører til fravær av regulering. Det er imidlertid viktig å være oppmerksom på den interesseavveining som må foretas mellom næringslivets interesser og den enkeltes personvern.

Målet med denne oppgaven var å gjøre en samlet vurdering av utfordringer knyttet til implementeringen av cookiedirektivet i norsk rett og hvordan direktivet kan gjennomføres. Blant utfordringene er tolkningen av kravet til samtykke etter personopplysningsloven og EU-direktivene. Man må for det første komme til en felles forståelse av hva kravet til aktivt samtykke fra brukeren innebærer. Trolig må nettleserne gå over til å bruke "opt-inn"-løsninger for innstillinger som godtar lagring av tredjepartscookies. Videre vil det bli nødvendig å fastsette hvilke krav som må stilles til de behandlingsansvarliges informasjonsplikt, både gjennom personvernpolicyer og generell informasjon på nettsider.

---

[191] Apenes (2010) s. 119.

En annen utfordring ligger i å finne tekniske løsninger som ved sin arkitektur fremmer personvernet. Det er flere mulige måter å gjøre dette på. Utviklingen og implementeringen av slike løsninger er allerede i gang, blant annet ved W3C sin innsats for å standardisere "Do Not Track"-spesifikasjonen. Det er imidlertid også viktig å gi spillerom for utvikling av nye løsninger. I IT-bransjen er endring den eneste konstanten, og det er viktig å være oppdatert på endringene som skjer. Videre har tilsynsmyndighetene et ansvar for å legge til rette for kommunikasjon mellom lovgiverne og næringslivet. En god dialog mellom lovgiverne, tilsynsmyndighetene, IT-bransjen og reklamebransjen vil bli uvurderlig i arbeidet med å implementere cookiedirektivet. Det vil også være viktig å søke å harmonisere reglene om lagring av cookies mellom de enkelte landene, blant annet slik at de store, internasjonale næringslivsaktørene får et mest mulig samlet regelsett å forholde seg til. En internasjonal harmonisering vil også kunne bidra til at de behandlingsansvarlige ikke har muligheter til å finne "smutthull" for ulovlig behandling av personopplysninger.

Vi må søke å harmonisere enkeltindividets interesser og næringslivets interesser i størst mulig grad. I dette ligger et behov for harmonisering av lovregler og teknologi. For at lovreglene skal kunne implementeres, må man ha teknologi som tillater dette. Men for at vi skal sikre utviklingen av personvernfremmende teknologiske løsninger, må slike løsninger også kreves etter loven.

7 Litteraturliste

Bøker:

Blixrud, Katrine Berg og Christine Ask Ottesen. *Personvern i finanssektoren*. 1. Utgave. Oslo (Gyldendal Akademisk), 2010.

Cannon, J.C. *Privacy. What Developers and IT Professionals Should Know*. Boston (Addison-Wesley), 2005.

Coll, Line M. og Clude A. Lenth. *Personopplysningsloven – en håndbok.* 1. Utgave. Oslo (Kommuneforlaget), 2000.

Data Protection in a Profiled World (2010). Redigert av Serge Gutwirth …[et al.]. 1. utg. Dordrecht (Springer), 2010.

Johansen, Michal Wiik, Knut Brede Kaspersen og Åste Marie Berseng Skullerud. *Personopplysningsloven kommentarutgave*. 1. Utgave. Oslo (Universitetsforlaget), 2001.

Lessig, Lawrence. *Code, version 2.0*. 1. Utgave. New York (Basic Books), 2006.

Mestad, Ingvild. *Elektroniske spor: nye perspektiver på personvern*. Oslo (Universitetsforlaget), 1986.

Rasmussen, Terje. *Kampen om internett*. 1. Utgave. Oslo (Pax), 2007.

Schartum, Dag Wiese og Lee A. Bygrave. *Utredning av behov for endringer i personopplysningsloven: skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet*. Oslo (Justis- og politidepartementet), 2006.

Schartum, Dag Wiese og Lee A. Bygrave. *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger.* 2. Utgave. Bergen (Fagbokforlaget), 2011.

Artikler:

Apenes, Georg. *Kampen for personvernet. Om kampen for tillitssamfunnet.* I: Clemet, Kristin og Egeland, John O.: *Til forsvar for personvernet*. Oslo (Universitetsforlaget), 2010.

Direktoratet for forvaltning og IKT. *Evaluering av Datatilsynet. Rapport 2011:8.* Oslo (Difi), 2011.

Dwyer, Catherine. *Behavioural Targeting: A Case Study of Consumer Tracking on Levis.com.* Association for Information Systems. The Americas Conference on Information Systems 2009 Proceedings (2009).

Simons, Frank, Gerrit-Jan Zwenne and Feyo Sickinghe. *The Netherlands: Consent for tracking cookies still a hot topic.* Privacy Laws & Business International Report, utg. 112 September (2011).

Sipior, Janice C., Burke T. Ward and Ruben A. Mendoza. *Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons*. Journal of Internet Commerce. 10 (2011). S. 1-16.

Lovgivning:

Norsk lovgivning:

1814 Kongeriget Norges Grundlov (Grunnloven) av 17. Mai 1814.

1918 Lov om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer (avtaleloven) av 31. mai 1918 nr. 4.

1972 Lov om strafferegistrering (strafferegistreringsloven) av 11. Juni 1971 nr. 52.

2000 Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr. 31.

2001 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) av 18. Mai 2001 nr. 24.

2003 Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven) av 23. mai 2003 nr. 35.

2003 Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 nr. 83.

2004 Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) av 16. februar 2004 nr. 401.

Traktater:

2004/C 310/01– Treaty establishing a Constitution for Europe (*EU-grunnloven*).

EU-Direktiver:

31995L0046 – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*Personverndirektivet*).

32002L0058 – Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (*Kommunikasjonsverndirektivet*).

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance (*Cookiedirektivet*).

Utenlandsk lov:

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Loi Informatique et Libertés). (Den franske loven om elektronisk kommunikasjon).

Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques. (Den franske forskriften som implementerer cookiedirektivet).

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 No. 1208. (Den britiske loven om elektronisk kommunikasjon).

Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet). (Den nederlandske loven om telekommunikasjon).

Vedtak truffet av Personvernnemnda:

PVN-2003-01	Klage på Datatilsynets vedtak i sak om avslag på konsesjonssøknad for opprettelse av sentralt låneregister.
PVN-2006-04	Microsoft Windows XP. Klage på Datatilsynets vedtak om at saken ikke strider mot personopplysningsloven med forskrift.
PVN-2009-14	Altinn. Klage på Datatilsynets vedtak om at Altinn sentralforvaltning må avslutte logging av fødselsnummer og tilhørende IP-adresse.

PVN-2009-16	Drosjeløyve. Klage på Datatilsynets vedtak om at Oslo kommune ikke kan be om samtykke fra løyvesøker til å innhente vandelsopplysninger ved tildeling av drosjeløyver, samt pålegg om sletting av innhentede personopplysninger.
PVN-2010-09	Ung i Norden. Klage på Datatilsynets delvise avslag på søknad om konsesjon til å behandle personopplysninger i forskning.

Forarbeider:

NOU 1997:19	Et bedre personvern - forslag til lov om behandling av personopplysninger.
NOU 2005:1	God forskning - bedre helse. Lov om forskning og helsefaglig forskning, som involerer mennesker, humant biologisk materiale og helseopplysninger (helseforskningsloven).
Ot.prp.nr 92 (1998-1999).	Om lov om behandling av personopplysninger (personopplysningsloven).
Ot.prp.nr 31 (2002-2003)	Om lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven).
Ot.prp.nr 58 (2002-2003).	Om lov om elektronisk kommunikasjon (ekomloven).

Artikkel 29-arbeidsgruppen:

Article 29 Data Protection Working Party. *Letter from the Article 29 Working Party adressed to Online Behavioural Advertising (OBA) Industry regarding self-regulatory Framework.* Brüssel, 3. august 2011.

Article 29 Data Protection Working Party. WP 37: *Privacy on the Internet – An integrated EU Approach to On-line Data Protection*. Brüssel, 12. juli 2000.

Article 29 Data Protection Working Party. WP 131: *Working document on the processing of personal data relating to health in electronic health records (EHR).* Brüssel, 15. februar 2007.

Article 29 Data Protection Working Party. WP 136: *Opinion 4/2007 on the concept of personal data*. Brüssel, 20. juni 2007.

Article 29 Data Protection Working Party. WP 171: *Opinion 2/2010 on online behavioural advertising.* Brüssel, 22. juni 2010.

Article 29 Data Protection Working Party. WP 187: *Opinion 15/2011 on the definition of consent*. Brüssel, 13. juli 2011.

Article 29 Data Protection Working Party. WP 148: *Opinion 1/2008 on data protection issues related to search engines.* Brüssel, 4. april 2008.

Alle arbeidsgruppens dokumenter er tilgjengelige her: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm [Sitert 24. November 2011].

Internett-dokumenter:

CNIL. *Transposition du Paquet télécom : renforcement des droits des internautes et signalement des failles de sécurité à la CNIL.* Det franske datatilsynets nettside om implementeringen av telekom-pakken (deriblant de nye cookiereglene), 2011. http://www.cnil.fr/la-cnil/actu-cnil/article/article/transposition-du-paquet-telecom-renforcement-des-droits-des-internautes-et-signalement-des-fail/ [sitert 11. november 2011]

EU-kommisjonen. *Digital Agenda: Commission starts legal action against 20 Member States on late implementation of telecoms rules.* Pressemelding 19. juli 2011. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/905&format=HTML&aged=0&language=EN&guiLanguage=en [Sitert 22. november 2011]

EUR-LEX [1]. informasjonsside om EU-direktivenes fortaler: http://eur-lex.europa.eu/en/techleg/10.htm [sitert 22. november 2011]

EUR-LEX [2]. *National provisions communicated by the member states concerning Directive 2009/136/EC (…).* Nettside med oversiktover implementeringsprosessene for cookiedirektivet i Eus medlemsland. November 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72009L0136:EN:NOT#FIELD_BE [Sitert 24. November 2011]

Europaportalen. *Endringer i ekompakken II.* EØS-notat fra nettsidene til Europaportalen, opprettet 27. november 2007. http://www.regjeringen.no/nb/sub/europaportalen/eos-notatbasen/notatene/2007/nov/revidert-uso-og-komverndirektiv.html?id=523434 [sitert 22. november 2011]

The European Advertising Standards Alliance (EASA) [1]. *EASA Best Practice Recommendation on Online Behavioural Advertising*. 13. april 2011. http://www.easa-alliance.org/page.aspx/162 [sitert 22. November 2011]

The European Advertising Standards Alliance (EASA) [2]. *European SRO members.* Kart over selvreguleringsorganisasjoner som er medlemmer i EASA, 2011. http://www.easa-alliance.org/About-EASA/EASA-Members/European-SRO-Members/page.aspx/55 [Sitert 23. November 2011]

Fleischer, Peter. *How long should Google remember searches?* Blogginnlegg for Google, 6. November 2007. http://googleblog.blogspot.com/2007/06/how-long-should-google-remember.html [sitert 22. november 2011]

Forbrukerombudet. *Utkast til endringer i ekomlov, ekomforskrift og nummerforskrift – høringsuttalelse*. 23. september 2010. http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2010/horing-om-endring-i-lov-om-elektronisk-k/horingsuttalelser.html?id=610270 [Sitert 23. november 2011]

Google Inc. *Third Quarter 2011 Financial Results.* 13. oktober, 2011. http://investor.google.com/earnings/2011/Q3_google_earnings.html [sitert 22. November 2011]

Henriksen, Øyvind [1]. *Ny norsk lov kan lamme internett*. Artikkel i E24 24. januar 2011. http://e24.no/media/ny-norsk-lov-kan-lamme-internett/4002960 [Sitert 10. november 2011]

Henriksen, Øyvind [2]: *EU-direktiv lager trøbbel: Nettbransjen om ekomforskriften: - Gammeldags, inkompetent og næringsfiendtlig*. Artikkel i E24 25. januar 2011. http://e24.no/media/nettbransjen-om-ekomforskriften-gammeldags-inkompetent-og-naeringsfiendtlig/4004411?view=print [Sitert 10. november 2011]

Information Commissioner's Office [1]. *Advice on the New Cookies Regulations*. 9. mai 2011. http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/cookie_rules_prepare.aspx [Sitert 11. november 2011]

Information Commissioner's Office [2]. *Enforcing the revised Privacy and Electronic Communications Regulations (PECR).* 25. mai 2011. http://www.ico.gov.uk/news/current_topics/new_pecr_rules.aspx [sitert 22. November 2011]

INMA og Mediebedriftenes landsforening. *Endringer i ekomforskriften vedrørende informasjonskapsler ("cookies").* Høringsuttalelse, Oslo, 25. januar 2011. http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2010/horing-om-endring-i-lov-om-elektronisk-k/horingsuttalelser.html?id=610270 [sitert 23. November 2011]

INMA. *Hvordan blir internett ifølge den nye cookiereguleringen?* 2011. http://www.inma.no/artikler/fagartikler/hvordan-blir-internett-ifolge-den-nye-cookiereguleringen [Sitert 8. november 2011]

IT- og Telestyrelsen. *Nye cookie-regler fra EU kræver nærmere afklaring*. Artikkel fra IT- og Telestyrelsens nettsider. 06. juni 2011. http://www.itst.dk/sikkerhed/privacy/lagring-af-og-adgang-til-oplysninger-pa-andres-udstyr/nye-cookie-regler-fra-eu-krever-nermere-afklaring [Sitert 11. november 2011]

IT-sikkerhedskomiteen. *Privatliv og/eller marked i en digital verden?* Notat fra It-sikkerhedskomiteens konferanse om privatliv og marked i en digital verden. 2. mars 2011. http://www.itst.dk/sikkerhed/fora/it-sikkerhedskomiteen/konferencer-og-arrangementer/konference-privatliv-og-marked-i-en-digital-verden [sitert 11. november 2011]

Jensen, Carlos og Potts, Colin. *Privacy policies as decision-making tools: an evaluation of online privacy notices*. Paper til The CHI '04 Proceedings of the SIGCHI conference on Human factors in computing systems. Wien (CHI 2004), 24.-29. april 2004. http://dl.acm.org/citation.cfm?id=985752 [sitert 22. november 2011]

Kamkar, Samy. *Evercookie – never forget.* 11. oktober 2010. http://samy.pl/evercookie/ [Sitert 23. November 2011]

Kroes, Neelie. *Online privacy – reinforcing trust and confidence.* Tale gjengitt i pressemelding, 22. juni 2011. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/461 [sitert 23. November 2011]

Miller, John W. *EU's Push on Internet Cookies Fizzles Out*. Artikkel i Wall Street Journals nettutgave. 17. januar 2011. http://online.wsj.com/article/SB10001424052748703396604576087992755049156.html?mod=WSJ_Tech_LEFTTopNews [Sitert 10. november 2011]

Ministeriet for Videnskab, Teknologi og Udvikling [1]. *Udkast til bekendtgørelse om krav til information og samtykke ved lagring af og adgang til oplysninger i slutbrugeres terminaludstyr*. 1. mars 2011. https://www.borger.dk/Lovgivning/Hoeringsportalen/Sider/Fakta.aspx?hpid=2146002415 [Sitert 11. November 2011]

Ministeriet for Videnskab, Teknologi og Udvikling [2]. *Høringsbrev*. 1. mars 2011. https://www.borger.dk/Lovgivning/Hoeringsportalen/Sider/Fakta.aspx?hpid=2146002415 [sitert 11. november 2011]

Post- og teletilsynet. *Høringssvar fra Post- og teletilsynet – Samferdselsdepartementets forslag til endringer i ekomloven, ekomforskriften og nummerforskriften.* 24. september 2010. http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2010/horing-om-endring-i-lov-om-elektronisk-k/horingsuttalelser.html?id=610270 [Sitert 23. november 2011]

Samferdselsdepartementet. *Høring om endring i lov om elektronisk kommunikasjon med forskrifter.* Nettside for saksgangen til forslag om endringer i ekomlov, ekomforskrift og nummerforskrift. Oslo (Samferdselsdepartementet), 2010. http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2010/horing-om-endring-i-lov-om-elektronisk-k/Horingsnotat.html?id=610271 [sitert 19. November 2011]

Schwartz, John. *Giving the Web a Memory Cost Its Users Privacy*. Artikkel i The New York Times, 4. september 2011. http://www.nytimes.com/2001/09/04/technology/04COOK.html[Sitert 24. november 2011]

Talberg-Furulund, Trude. *Anbefaler Europarådet å utvikle systemer med personverngaranti.* Datatilsynet, 2010. http://www.datatilsynet.no/templates/Page___3700.aspx [sitert 18. november 2011]

Tirtea, Rodica, Claude Castelluccia and Demosthenes Ikonomou. *Bittersweet cookies. Some security and privacy considerations.* Rapport for European Network and Information Security Agency (ENISA) 2. februar 2011. http://www.enisa.europa.eu/act/it/library/pp/cookies [sitert 19. November 2011]

W3C. *W3C Announces First Draft of Standard for Online Privacy*. 14. november 2011. http://www.w3.org/2011/11/dnt-pr.html.en [Sitert 17. november 2011]

Personlige meddelelser:

Willstedt, Anders. E-post. 14. november 2011.

Wongraven, Eli. E-post. 7. november 2011.

Generelle nettsider (Informasjonssider osv.):

www.cnil.fr
Nettsiden til det franske datatilsynet.

www.datatilsynet.no

Nettsiden til det norske Datatilsynet.
http://donottrack.us/
Informasjonsside om "Do Not Track"-spesifikasjonen, moderert av spesifikasjonens utviklere.

http://www.easa-alliance.org/
Nettsiden til EASA.

www.forbrukerombudet.no
Nettsiden til det norske Forbrukerombudet.

http://www.google.no/intl/en/ads/
Googles hjemmeside for sine reklametjenester.

http://www.google.com/analytics/
Informasjonsside for Google Analytics.

http://www.google.com/intl/en/privacy/
Hjemmesiden til Googles personvernpolicy.

http://www.iabeurope.eu/
Nettsiden til IAB Europe.

www.ico.gov.uk
Nettsiden til det britiske datatilsynet.

http://www.inma.no/
Nettsiden til INMA.

www.npt.no
Nettsiden til det norske Post- og teletilsynet.

http://www.opta.nl/en/
Nettsiden til det nederlandske datatilsynet.

8 Lister over tabeller og figurer m v

Figur 1 Hvordan fungerer cookies?

Figur 2 Forskjellige typer cookies i et personvernperspektiv.